APCERT Annual Report 2011

APCERT Secretariat
E-mail: apcert-sec@apcert.org URL: http://www.apcert.org

APCERT
Asia Pacific Computer Emergency Response Team

CONTENTS

Chair's Message 2011

After 9 years of successful collaboration and activities, APCERT updated its vision at the last Annual General Meeting in March 2011. Our new vision is "APCERT will work to help create a Safe, Clean and Reliable Cyber Space in the Asia Pacific Region through global collaboration." Each member CSIRT serves its own constituency for security incident response and information infrastructure protection and APCERT members support each other to achieve that mission through membership in APCERT and participation in its forums and activities. APCERT also increasingly serves as a regional collaboration forum for members to work together and collaborate globally to improve the health and security of our shared common environment – the Internet. We must begin to implement strategies and approaches that work to improve the Internet ecosystem and its health in addition to protecting against and reacting to specific threats and incidents.

The APCERT members realize the need to jointly work and that global efforts are required to solve common cyber security challenges. We plan to contribute to making the Internet ecosystem cleaner and healthier as a basis for improved cyber security in the Asia Pacific as a mutual gain for all in the long-term. As a step, we participated global dialogues to discuss clean-up norms, signed MOU with Organization of Islamic Cooperation in September, kept closed engagement with other regional CERT frameworks, and AP regional policy frameworks and operation groups.

This year, our activities also focused on improving APCERT as a collaboration forum. After 9 years since its formation, we know we face new threats, CERTs and other key stake holders relationships are evolving as security operations community acts globally and regionally, and therefore collaboration with these and other key stakeholders becomes ever more critical for our situation awareness and effective incident response. Hence, members worked through the Working Group to discuss new membership structure, new mechanism to energize the information sharing and collaboration among members and also with global/regional security operations and experts. Steering committee and Working Group conveners have conducted the membership survey, prioritized the problem areas and developed the next steps for

improvement.

APCERT will lead and move forward. We have built trust and strong collaboration with each other. Now we must deepen that collaboration and work with others to extend our efforts make cyberspace more safe and secure. I look forward to working with you all and our partners across the globe to make next year our most successful!

Yurie Ito,
Chair, APCERT
Director, Global Coordination Division, JPCERT/CC

I. About APCERT

1. Objectives and Scope of Activities

APCERT *(Asia Pacific Computer Emergency Response Team)* is a coalition of the forum of CERTs *(Computer Emergency Response Teams)* and CSIRTs *(Computer Security Incident Response Teams)*. The organization was established on February 2003 to encourage and support the activities of CERTs/CSIRTs in the Asia Pacific region.

APCERT will maintain a trusted contact network of computer security experts in the Asia-pacific region to improve the regions' awareness and competency in relation to computer security incidents through:

1. enhancing Asia-Pacific regional and international cooperation on information security;
2. jointly developing measures to deal with large-scale or regional network security incidents;
3. facilitating information sharing and technology exchange, including information security, computer virus and malicious code, among its members;
4. promoting collaborative research and development on subjects of interest to its members;
5. assisting other CERTs and CSIRTs in the region to conduct efficient and effective computer emergency response;
6. providing inputs and/or recommendations to help address legal issues related to information security and emergency response across regional boundaries.

The formation of CERTs/CSIRTs at the organizational, national and regional levels is essential to the effective and efficient response to computer security incidents, widespread security vulnerabilities and incident coordination throughout the region. One important role of CERTs/CSIRTs is education and training to raise awareness and encourage best practice. APCERT coordinates activities with other regional and global organizations, such as the Forum of incident Response and Security Teams (FIRST) <www.first.org>, and TF-CSIRT, a task force that promotes collaboration between CSIRTs at the European level <www.terena.nl/tech/task-forces/tf-csirt/>.

The geographical boundary of APCERT activities are the same as that of APNIC. The region covers the entire Asia-Pacific, comprising of 56 economies. The list of those economies is available at:

http://www.apnic.net/about-APNIC/organization/apnics-region

At present, APCERT Chair is JPCERT/CC (Japan Computer Emergency Response Team/Coordination Center). Deputy Chair is KrCERT/CC (Korea Internet Security Center). JPCERT/CC (Japan Computer Emergency Response Team/Coordination Center) serves as secretariat.

URL: http://www.apcert.org
Email: apcert-sec@apcert.org.

2. APCERT Members

APCERT was formed in 2003 by 15 teams from 12 economies across the Asia-Pacific region, and has increased its membership since then. In 2010, TechCERT, MonCIRT and CERT Australia have been approved as General Member of APCERT. Also, BruCERT has upgraded its membership to Full Member of APCERT.
As of December 2011, APCERT consists of 28 teams from 19 economies across the AP region, of which 19 teams are full members and 9 teams are general members.

Full Members

Team	Official Team Name	Economy
AusCERT	Australian Computer Emergency Response Team	Australia
Bkis	Bach Khoa Internetwork Security Center	Vietnam
BruCERT	Brunei Computer Emergency Response Team	Negara Brunei Darussalam
CCERT	CERNET Computer Emergency Response Team	People's Republic of China

CERT-In	Indian Computer Emergency Response Team	India
CNCERT/CC	National Computer network Emergency Response technical Team / Coordination Center of China	People's Republic of China
HKCERT	Hong Kong Computer Emergency Response Team Coordination Centre	Hong Kong, China
ID-CERT	Indonesia Computer Emergency Response Team	Indonesia
ID-SIRTII	Indonesia Security Incident Response Team of Internet Infrastructure	Indonesia
JPCERT/CC	Japan Computer Emergency Response Team / Coordination Center	Japan
KrCERT/CC	Korea Internet Security Center	Korea
MyCERT	Malaysian Computer Emergency Response Team	Malaysia
PHCERT	Philippine Computer Emergency Response Team	Philippine
SingCERT	Singapore Computer Emergency Response Team	Singapore
Sri Lanka CERT/CC	Sri Lanka Computer Emergency Readiness Team Coordination Centre	Sri Lanka
ThaiCERT	Thai Computer Emergency Response Team	Thailand
TWCERT/CC	Taiwan Computer Emergency Response Team / Coordination Center	Chinese Taipei
TWNCERT	Taiwan National Computer Emergency Response Team	Chinese Taipei
VNCERT	Vietnam Computer Emergency Response Team	Vietnam

General Members

Team	Official Team Name	Economy
BDCERT	Bangladesh Computer Emergency Response Team	Bangladesh
BP DSIRT	BP Digital Security Incident Response Team	Singapore
CERT Australia	CERT Australia	Australia
GCSIRT	Government Computer Security and Incident Response Team	Philippines
mmCERT	Myanmar Computer Emergency Response Team	Myanmar
MOCERT	Macau Computer Emergency Response Team Coordination Centre	Macao

MonCIRT	Mongolian Cyber Incident Response Team	Mongolia
NUSCERT	National University of Singapore Computer Emergency Response Team	Singapore
TechCERT	TechCERT	Sri Lanka

3. Steering Committee (SC)

Since the last APCERT AGM held in March 2010, in Jeju, Korea, the following members served as APCERT Steering Committee (SC).

- JPCERT/CC (Chair/Secretariat)
- KrCERT/CC (Deputy Chair)
- AusCERT
- HKCERT
- MyCERT
- SingCERT
- ThaiCERT

4. Working Groups (WG)

There are 5 Working Groups in APCERT.

1) TSUBAME WG (formed in 2009)

- Objectives:
  - Establish a common platform for Internet threat monitoring, information sharing & analyses in Asia-Pacific region
  - Promote collaboration among CSIRT in Asia-Pacific region by using the common platform
  - Enhance capability of global threat analyses by incorporating 3D Visualization features to the common platform
- Members: JPCERT/CC (secretariat) and TSUBAME project members
- Status: Active; Held TSUBAME Workshop in 2011

2) Information Classification WG (formed in 2011)

- Objective: To devise an appropriate information classification and handling system to be adopted for use by APCERT members when communicating or sharing information with each other
- Convener: Kathryn Kerr (AusCERT)
- Status: Active;

3) Information Sharing WG (formed in 2011)

- Objective: To identify different types of information that is regarded as useful for APCERT members to receive and/or which is available to share with other APCERT members.
- Convener: Yonglin Zhou (CNCERT/CC)
- S t a t u s : Active;

4) Membership WG (formed in 2011)

- Objective: To review the current membership criteria/classes and determine whether they should be broadened to include new criteria/classes and if so how should the new arrangements work.
- Convener: Jinhyun Cho (KrCERT/CC)
- S t a t u s : Active;

5) Operational Framework WG (formed in 2011)

- Objective: To identify changes that need to be made to the existing APCERT Operational Framework
- Convener: Roy Ko (HKCERT)
- S t a t u s : Active;

5. APCERT Website

JPCERT/CC manages and updates the APCERT website <www.apcert.org>.
On a temporary basis, AusCERT hosts the Point of Contact (POC) information for APCERT POC teams. Access is by password only for APCERT teams.

II. APCERT Activity Report 2011

1. International Activities and Engagements

APCERT has been active in representing and promoting APCERT in various international events. From January 2011 to December 2011, APCERT members have hosted, participated and/or contributed in the following events:

- **APCERT Drill 2011**

  http://www.apcert.org/documents/pdf/Drill2011_PressRelease.pdf

  On 22 February, APCERT Drill 2011, the 7th APCERT Cyber Exercise Drill, was successfully held with participation from 20 teams of 15 economies (Australia, Brunei, Bangladesh, China, Chinese Taipei, Hong Kong, India, Indonesia, Japan, Korea, Malaysia, Singapore, Sri Lanka, Thailand, and Vietnam). The theme of the drill was "Critical Infrastructure Protection" and was coordinated by SLCERT (Leader of the Organizing .Committee), TechCERT (Leader of the Exercise Control), CERT Australia, VNCERT, BKIS with advices from HKCERT and MYCERT.

- **APCERT AGM & Conference 2011**

  The APCERT Annual General Meeting (AGM) & Conference 2011 took place in Lotte Hotel Jeju, Jeju Island, Korea, from 23-24 March, hosted by KrCERT/CC.

  The event brought together 19 team-representatives from 15 economies, and also guest speakers from other regions and local audiences.

  The overall program of the event was as follows:

  - 23 March Morning: AGM
  - 23 March Afternoon: Conference (Closed to APCERT members and invited guests)
  - 24 March Full-day: Conference (Open to public)

  The event was successful in providing a productive platform for fruitful discussions on strategic planning on APCERT's operation. After a very intensive discussion during the AGM, a new vision of APCERT has been approved among the members: "APCERT will work to create a safe, clean and reliable cyber space in the Asia Pacific region through global collaboration."

The event also provided opportunities for the teams to share information on trends of information security and some best practices of CSIRTs inside/outside the region.

- **APCERT Workshop 2011 - TSUBAME Network Traffic Monitoring Project**

  APCERT Workshop 2011 on TSUBAME Network Traffic Monitoring Project, was held in the morning of 25 March, in conjunction with APCERT AGM & Conference 2011. The workshop was organized by JPCERT/CC to enhance the TSUBAME project and the cooperation among its members.

- **CSIRT Trainings for AFRICA**

  JPCERT/CC organized trainings for African CSIRTs and introduced APCERT activities in this training on behalf of APCERT.

  - 30 May to 4 June, Dar es Salaam, Tanzania
  - 19-22 November, Yaounde, Cameroon

- **The Second Worldwide Cybersecurity Summit**

  The Second Worldwide Cybersecurity Summit organized by the EastWest Institute (EWI) was held in London from 1-2 June. There, Ms. Yurie Ito, the Chair of APCERT, joined the poster session, giving explanation on "Asia Pacific Regional Collaboration Activities in Making the Internet Clean, Safe and Reliable".

- **Annual National CSIRT Meeting**

  Annual National CSIRT Meeting hosted by the CERT Coordination Center was held in Vienna from 18-19 June. There, Ms. Yurie Ito, the Chair of APCERT, delivered a presentation entitled "Asia Pacific Regional Collaboration Activities in Making the Internet Clean, Safe and Reliable".

- **AP* Retreat Meeting**

  http://www.apstar.org/ap_retreat.php

  AP* is the community of Asia Pacific Internet organisations, with the vision to provide a strong united front for all Asia Pacific Internet organizations to deal with international issues of governance, administration, management, research, development, education and public awareness of the Internet. The AP*Retreat

Meeting, where organizations in the Asia Pacific region report and update their activities, was held in Busan on 2 September 2. There, Mr. Jinhyun Cho, the Deputy Chair of APCERT delivered a presentation entitled "APCERT Activities".

- **ACID (ASEAN CERT Incident Drill) 2011**

ACID (ASEAN CERT Incident Drill) 2011, lead and coordinated by SingCERT, entered its sixth iteration this year with participation from ASEAN CERTs and APCERT Teams. The drill was completed successfully with focus on detection and investigation of attacks using common file formats as transmission vectors for exploit.

- **APEC TEL 44**

The meeting for Security and Prosperity Steering Group (SPSG) of the APEC-TEL was held in Kuala Lumpur on 27 September. There, Ms. Yurie Ito, the Chair of APCERT, delivered a presentation via video entitled "Introducing APCERT New Vision".

- **MOU between APCERT and OIC-CERT**

http://www.apcert.org/documents/pdf/Joint-media-release-OIC-APCERT.pdf

APCERT and the Organisation of the Islamic Conference – CERT (OIC-CERT), has come to an agreement for the collaborative efforts amongst the OIC member countries and Asia Pacific region. The signing ceremony of this MOU was held on 27 September during the OIC-CERT Annual Conference 2011 in Dubai. Ms. Yurie Ito, the Chair was the signer.

- **The 2nd APT Cybersecurity Forum**

http://www.aptsec.org/2011-CSF

The 2nd APT Cybersecurity Forum, organized by the Asia Pacific Telecommunity and hosted by the Government of Japan, was held from 5-7 December in Tokyo, Japan.

Ms. Kaori Umemura of JPCERT/CC represented APCERT at this forum and presented on APCERT activities to the relevant participants.

Other International Activities and Engagements

- **DotAsia**

  APCERT was invited to be a member of the Advisory Council of DotAsia, to assist DotAsia in policy development and relevant community projects. HKCERT represented APCERT in attending the meetings of the Advisory Council.

- **FIRST (Forum of Incident Response and Security Teams)**

  Dr. Suguru Yamaguchi of JPCERT/CC is serving as Steering Committee member of FIRST from June 2011.

2. Approval of New General Members / Full Members

From January 2011 to December 2011, the following teams newly joined APCERT General Member / Full Member.

- MOCERT (Macao) was approved as General Member as of 4 March
- Id-SIRTII (Indonesia) was approved as Full Member as of 4 March
- mmCERT (Myanmar) was approved as General Member as of 7 December

3. APCERT SC Meetings

From January 2011 to December 2011, SC members held 1 face-to-face meeting and 7 teleconferences to discuss on APCERT operations and activities.

11 February	Teleconference
4 March	Teleconference
22 March	Face-to-face meeting
20 April	Teleconference
8 June	Teleconference
10 August	Teleconference
13 October	Teleconference
7 December	Teleconference

4. APCERT Survey 2011

To assess the APCERT's members' level of satisfaction with a range of aspects in the way that APCERT operates and functions, APCERT Steering Committee conducted a questionnaire survey from June to July. The summary and analysis of the survey was issued in August and is being used as a base document for future strategic planning by the Steering Committee and the Working Groups.

III. Activity Reports from APCERT Members

Full Members

1. AusCERT Activity Report

Australian Computer Emergency Response Team - Australia

About AusCERT

Introduction

AusCERT is the premier Computer Emergency Response Team (CERT) in Australia and a leading CERT in the Asia/Pacific region. AusCERT operates within a worldwide network of information security experts to provide computer incident prevention, response and mitigation strategies for members and assistance to affected parties in Australia. As a not-for-profit, self-funded organisation based at The University of Queensland, AusCERT relies on member subscriptions to cover its operating costs.

Establishment

AusCERT was the first Australian CSIRT and is one of the oldest CSIRTs, having been in continuous operation since 1993. AusCERT is on the steering committee of APCERT and is a member of FIRST.

Staffing

AusCERT has 13 staff members, including technical, administrative and managerial staff.

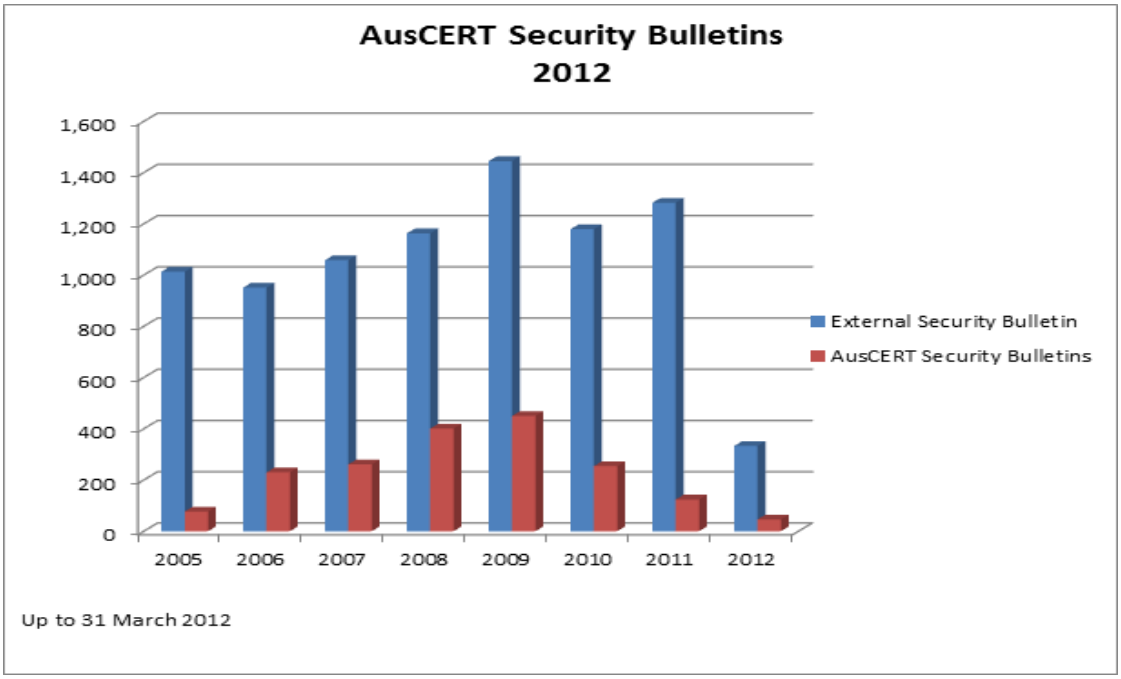
Constituency

AusCERT provides services to the Australian Internet community.

Activities and operations of AusCERT

Security advisories and bulletins

AusCERT distributes security advisories and bulletins to its members by email and publishes them to its website.

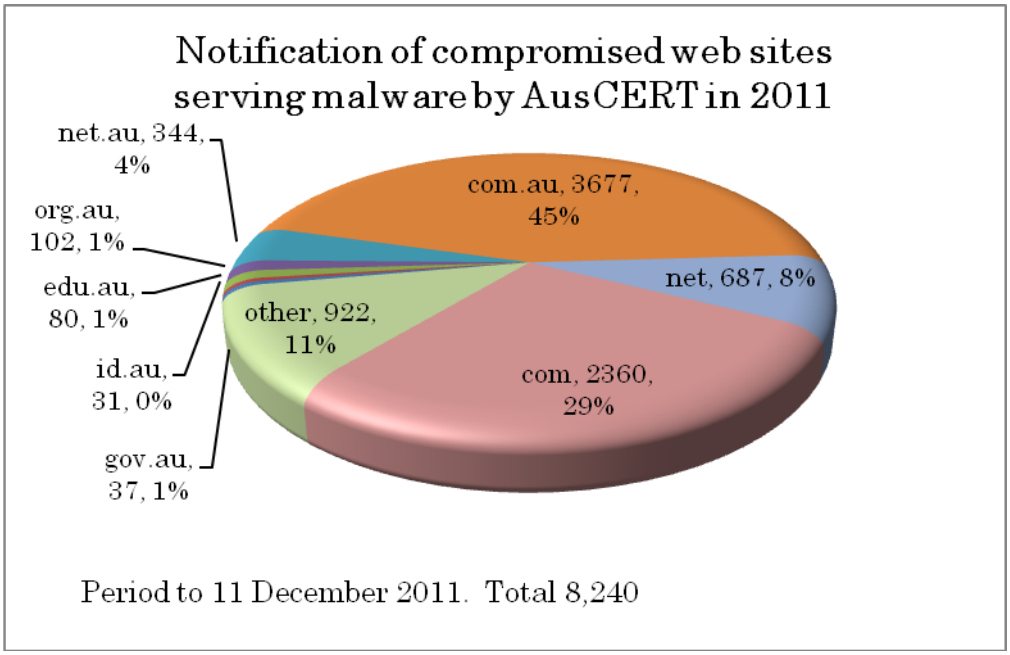


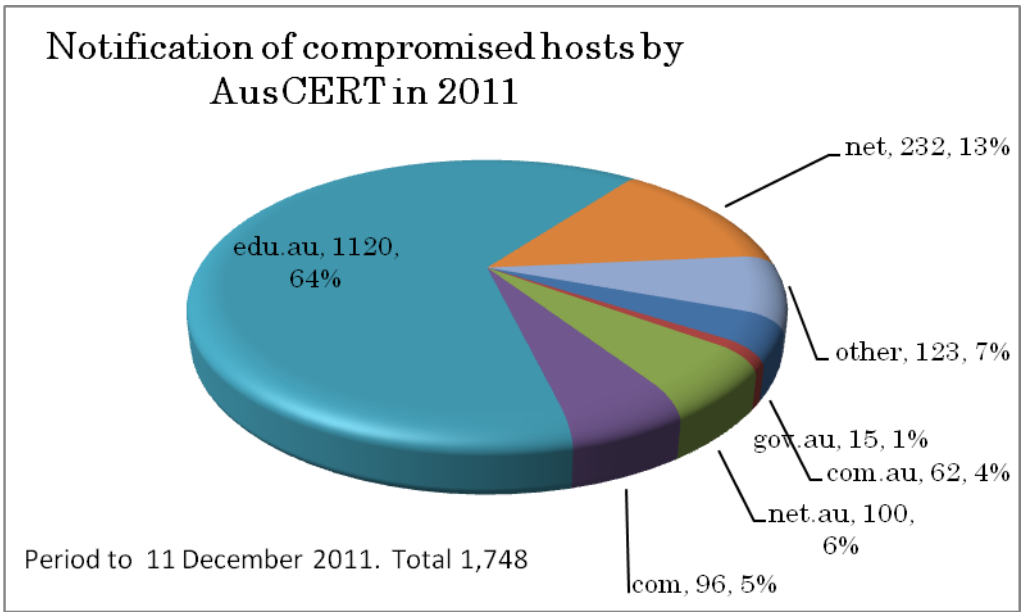
Incident response

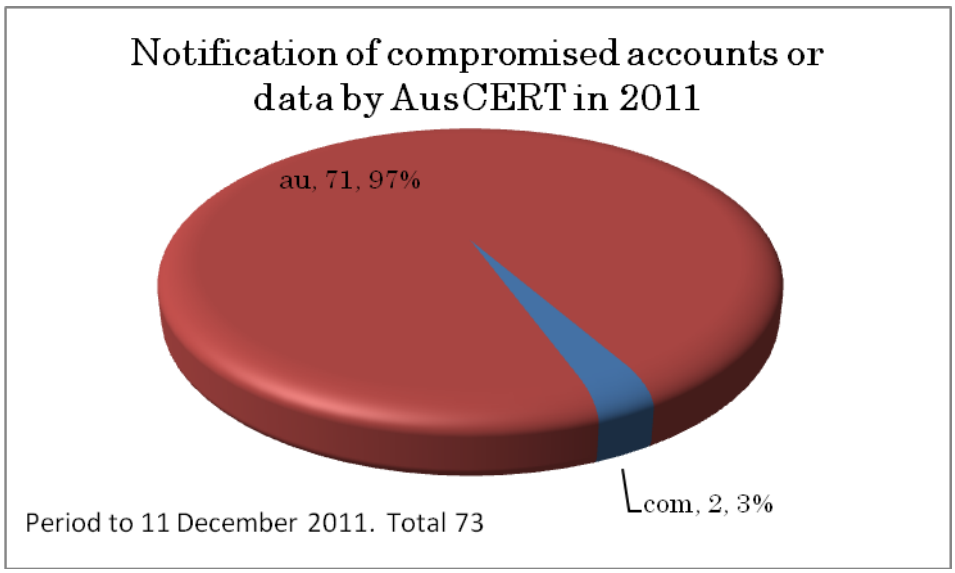
AusCERT coordinates incident response on behalf of its members and generates pro-active reports of incident activity, based on its data collection activities. Weekly, AusCERT provides a report to each of its members that details activity that affected the member for that week.

Compromise evidence collection and data distribution

AusCERT notified the community of compromise of their web sites, hosts and accounts in 2011.

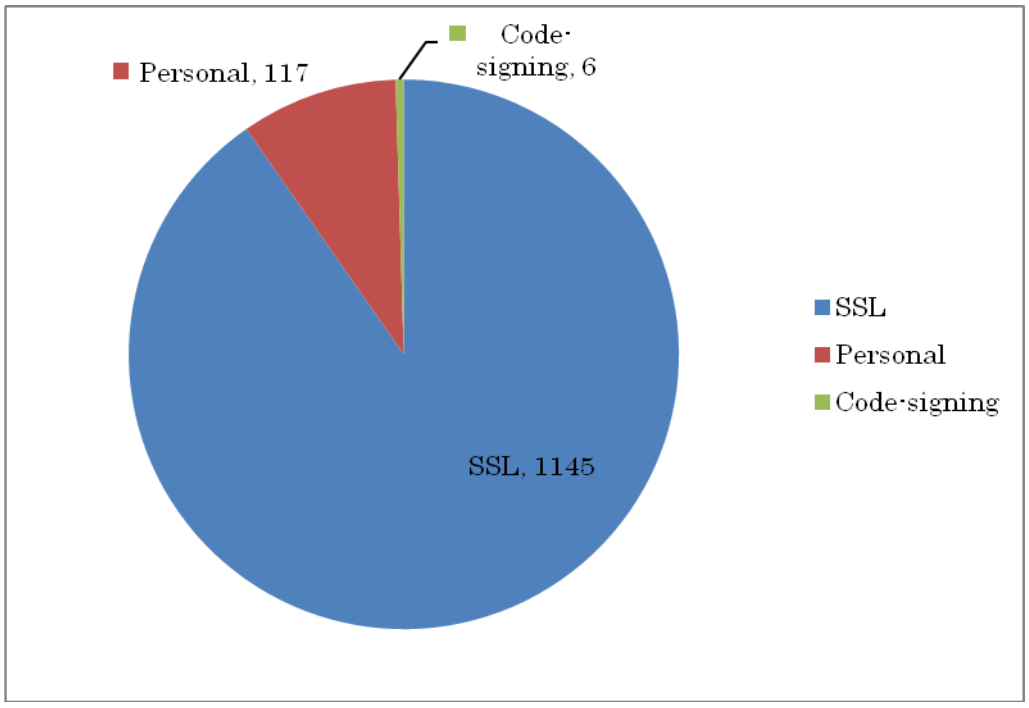

Notification of compromised web sites serving malware by AusCERT in 2011
net.au, 344, 4%
org.au, 102, 1%
edu.au, 80, 1%
id.au, 31, 0%
gov.au, 37, 1%
com.au, 3677, 45%
net, 687, 8%
other, 922, 11%
com, 2360, 29%
Period to 11 December 2011. Total 8,240


Notification of compromised hosts by AusCERT in 2011
net, 232, 13%
edu.au, 1120, 64%
other, 123, 7%
gov.au, 15, 1%
com.au, 62, 4%
net.au, 100, 6%
com, 96, 5%
Period to 11 December 2011. Total 1,748



Certificate service

AusCERT provides a PKI certificate service to the Australian higher education and research (HE&R) sector. This enables institutions to self-issue SSL, S/MIME and code-signing certificates at a discounted rate. Since October 2011, when the self-provisioning interface was released, AusCERT has issued a total of 1268 certificates.



Stay Smart Online Alert Service

In 2011, AusCERT operated the Australian Government funded Stay Smart Online Alert Service and provided security alerts, advisories and newsletters to the Australian Internet community under this banner.

Events

AusCERT security conference

AusCERT hosts an annual information security conference in Queensland, on the Gold Coast. It attracts international speakers and attendees and is the largest event of its type in the southern hemisphere.

http://conference.auscert.org.au

AusCERT Security on the Move

AusCERT, in partnership with SC Magazine, began hosting "Security on the Move", a one-day event that will rotate around major Australian capital cities.

Other events

AusCERT attended the following international events in 2011

- APCERT AGM and conference
- FIRST conference

AusCERT participated in the APCERT drill in February 2011.

Contacting AusCERT

AusCERT is contactable during Australian Eastern business hours and by its members 24x7.

Email: auscert@auscert.org.au

Web: http://auscert.org.au

Telephone: +61 7 3365 4417

2. BKIS Activity Report

Bach Khoa Internetwork Security Center – Vietnam

1.0 About Bkis - Vietnam

Bkis is a Vietnam's leading organization in researching, deploying network security software and solution. Bkis was established on December 28th, 2001, and became full member of APCERT in 2003.

Head Office: 5th Floor, Hitech Building, Hanoi University of Technology, 1A Dai Co Viet, Hanoi, Vietnam.

2.0 Activities & Operations

2.1 Security Statistics in Vietnam

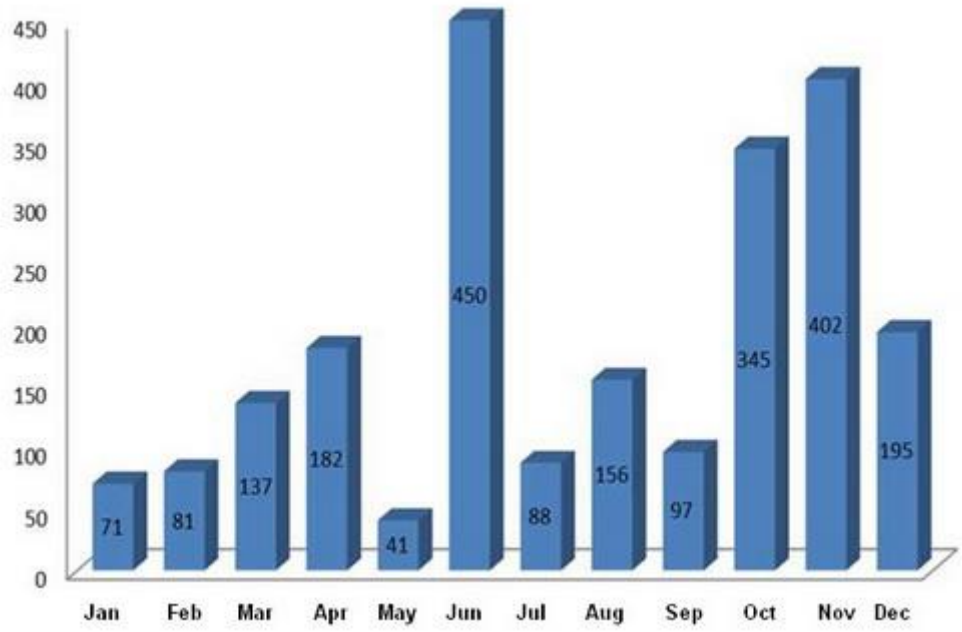
Overview of computer virus and network security in 2011:

According to statistics of Bkis HoneyPot, 64.2 million computers were infected by virus in 2011. In average, there were more than 175 thousands of computers infected each day.

In 2011, there were 38,961 newly emerging virus families, W32 Sality.PE was the most widespread virus, which infected approximately 4.2 million computers.

List of 15 most infectious viruses in 2011:

No	Name of virus
1	W32.Sality.PE
2	W32.AutoRunUSB.Worm
3	W32.Vetor.PE
4	W32.StuxnetQKY.Trojan
5	W32.StarterYY.Trojan
6	W32.Kawin.Trojan
7	W32.FakeUserinitIconF.Fam.Worm
8	X97M.XFSic
9	W32.SecretCNC.Heur
10	W32.SalDropFamA.Worm
11	W32.InjectAdwaredDwnMainA.Trojan
12	W32.Tmgrtext.PE
13	W32.CmVirus.Trojan
14	W32.SalDropE.Worm
15	W32.SysAntiA.Worm



The number of websites attacked in 2011

In 2011, about 2,245 Vietnamese enterprise's websites were attacked. In average 187 websites were assaulted each month.

The hidden danger of W32.Sality.PE network

More than 4.2 million computers were infected by metamorphic virus W32.Sality.PE in 2011, in average 11,000 new computers got infected with this virus each day. Sality penetrated in every Vietnamese computer networks. Bkis experts found Sality existence in almost all systems they checked. Sality is not only the most spreading virus in 2011, but also a "time bomb" which can explode and affect millions of computers in the near future.

According to Bkis experts, during their time of tracking the virus from 2009, despite of its infection on millions of computers, Sality keeps "staying still" and hasn't activated its destructive features like information stealing or data destroying. It's difficult to explain. There might be an organization or even a country which backs up the virus network and their intention is still a mystery.

A reason which makes W32.Sality.PE be able to spread to millions of computers is its ability of using genetic algorithms to automatically generate the next virus generations F1, F2…The longer the virus infects the computer, the more complex the variants get, making it increasingly hard for antivirus software to detect and disinfect. Therefore, W32.Sality.PE can bypass almost all antivirus software in the world.

Because of the seriousness of the problem, Bkis recommends that computer users should check their computers with antivirus software equipped with metamorphic virus disinfecting technique. Bkav users can use Bkav Pro to comprehensively remove this virus.

Phishing increased across social networks

By the end of 2010, Bkis experts predicted that many Internet phishing incidents would occur in 2011. It has happened. Bkis received more than 30 reports about phishing though Yahoo Messenger each month. In each event, the number of victims may reach ten. Despite being warned many times, a lot of users still lost their accounts or money due to their gullibility.

Besides Yahoo, now the biggest social network site, Facebook, has also become a tool for hackers. At the end of 2011, Bkis detected the first virus family which spread through Facebook chat. Comparing with virus in Yahoo Messenger, although Facebook virus doesn't have any new tricks, it still spreads rapidly thanks to the huge number of Facebook users. In addition, in social networks like Facebook or Twitter, there were series of famous people faking incidents in 2011.

Social networks and online chat programs have become effective tools for hackers. Once again, Bkis recommends that users should be careful when receiving information through Internet communicating channels. Especially, users need to be vigilant with received links or files. They should call their friends to check if their chatting accounts require money or other sensitive information.

Botnet and consecutive network attacks

2011 was a year of network attacks. There were consecutive attacks towards Vietnamese enterprise's networks with different methods. There were illegal penetrations to destroy database or deface websites. There were also DDoS attacks which made systems be paralytic in a long time. Many attacks aimed to rob domain names of enterprises. It was more dangerous that silent attacks happened with the installation of spy viruses to steal data from important organizations.

The attacks were mainly due to the lack of awareness about network security among the leaders of enterprises, organizations. This leads to wasteful investment and the lack of comprehensive solution for system security.

Specially, in 2011, more than 85,000 computers were installed Ramnit virus and stolen of important data. This shows the capability that the attacks may even influence a nation's security. Besides, this botnet was controlled by hackers through many servers in US, Russia, Germany, China to steal data from all over the world, not only in Vietnam. This is a popular situation in the world in 2011.

2.2 Threat landscape in 2012 in Vietnam

Rootkit will not be a privilege of some hackers like before, but will become a new trend once this tool is publicized. Metamorphic virus will employ more new techniques to prolong the spread for years.

Due to the popularity of Windows 7 which is able to ensure high security level, the important execution decision is up to the users. Thus, there would be an in increasing growth of virus designed to fool users' sense. Fake-icon virus is the first generation; and this trend is expected to continue in 2011.

Virus with socio-political motivation is to emerge more, taking advantage of popular software download websites to spread. Botnet which consists of the infected computers are used to perform attacks against targeted objects to steal confidential information from individuals and organizations.

More frauds and attacks against cell phones will occur in 2011. There may be first

assaults on cell phones to spread malicious codes, mainly in the form of hidden Trojan to steal users' personal information.

3.0 Events organized / co-organized

3.1 Training Courses

Network Security Training Courses:

Jun 2011: For Network Administrators from companies (Banks...)

Security Awareness Training Courses:

August 2011: 2 classes for Banks

3.2 Security Articles

In 2011, 20 security articles written by Bkis experts were posted on our security blog at security.bkis.vn.

3.3 Seminar

June 2011: Organized a seminar about security for e-government system.

December 2011: Organized a seminar on securing e-journal systems.

4.0 International Collaboration

February 2012: Bkis took part in the APCERT Drill as a member of the organizing committee and a member of the exercise control group

3. BruCERT Activity Report

Brunei Computer Emergency Response Team – Negara Brunei Darussalam

1.0 About BruCERT

1.1 Introduction

Brunei National Computer Emergency Response Team (BruCERT) was established in May 2004. It was formed in collaboration with AITI, the Ministry of Communication, to become the nation's first trusted one-stop referral agency in dealing with computer-related and internet-related security incidents in Brunei Darussalam.

The *Brunei Computer Emergency Response Team Coordination Centre (BruCERT)* welcome reports on computer security related incident. Any computer related security incident can be reported to us by:

Telephone: (673) 2458001
Facsimile: (673) 2458002
Email: cert@brucert.org.bn

1.1.1 BruCERT Services

- 24X7 Security Related Incidents and Emergency Response from BruCERT.
- 24X7 Security Related Incidents and Emergency Response onsite (Deployment response is within 2hrs after an incident is received). This service only applies to BruCERT Constituents.
- Broadcast alerts (Early Warning) of new vulnerabilities, advisories, viruses and Security Guidelines from BruCERT Website. BruCERT Constituents will receive alerts through email and telephone as well as defense strategies in tackling IT Security related issues.
- Promote Security Awareness program to educate and increase public awareness and understanding of information security and technical know-how through education, workshop, seminar and training.
- Coordinating with other CERT, Network Service Providers, Security Vendors, Government Agencies as well as other related organization to

facilitate the detection, analysis and prevention of security incidents on the internet.

1.1.2 BruCERT Workforce

BruCERT currently with strength of 44 Staff (100% local) and the rest is administration. BruCERT has undergone training on various IT security module, such as A+, N+, Linux+, Server+, Security+, SCNP, SCNA, CIW, CEH, CCNA, CISSP and BS7799 Implementer, where most of BruCERT workforce has gain certification in certain fields.

1.1.3 BruCERT Constituents

BruCERT has close relationship with Government agencies, 2 major ISPs and various numbers of vendors.

Government Agencies

Provide a security incident response services to national and government agencies as ITPSS is appointed as a central hub for all IT security-related issues across the nation and to become the Government trusted E-Security Advisor.

AITI

Authority for Info-communications Technology Industry of Brunei Darussalam (AITI) is an independent statutory body to regulate, license and develop the local ICT industry and manage the national radio frequency spectrum.

AITI has appointed ITPSS (Information Technology Protective Security Services), an IT local security company to become the national CERT in dealing with incident response in Brunei.

Royal Brunei Police Force

BruCERT has been collaborating with RBPF to resolve computer-related incidents.

TelBru – BruNet

TELBru, the main service provider of internet gateway. and BruCERT have been working together to engage information sharing of internet-related statistics and the current situation of IT environment in Brunei.

DST – simpur

The second largest internet service provider in Brunei.

2.0 BruCERT Activities and Operation in 2011

2.1 Incidents response

In 2011, BruCERT receive a few numbers of security incidents reports from the public even from the private sector. There were an increasing number of incidents that had been reported to BruCERT, which show positive feedbacks from the Brunei community. On the down side, there is also an increase number of website that had been defaced in Brunei. Most of the defacement are due to lack of security controls being placed and install security patches on the victims' sides. The statistic of the security incident is shown as Figure 1.

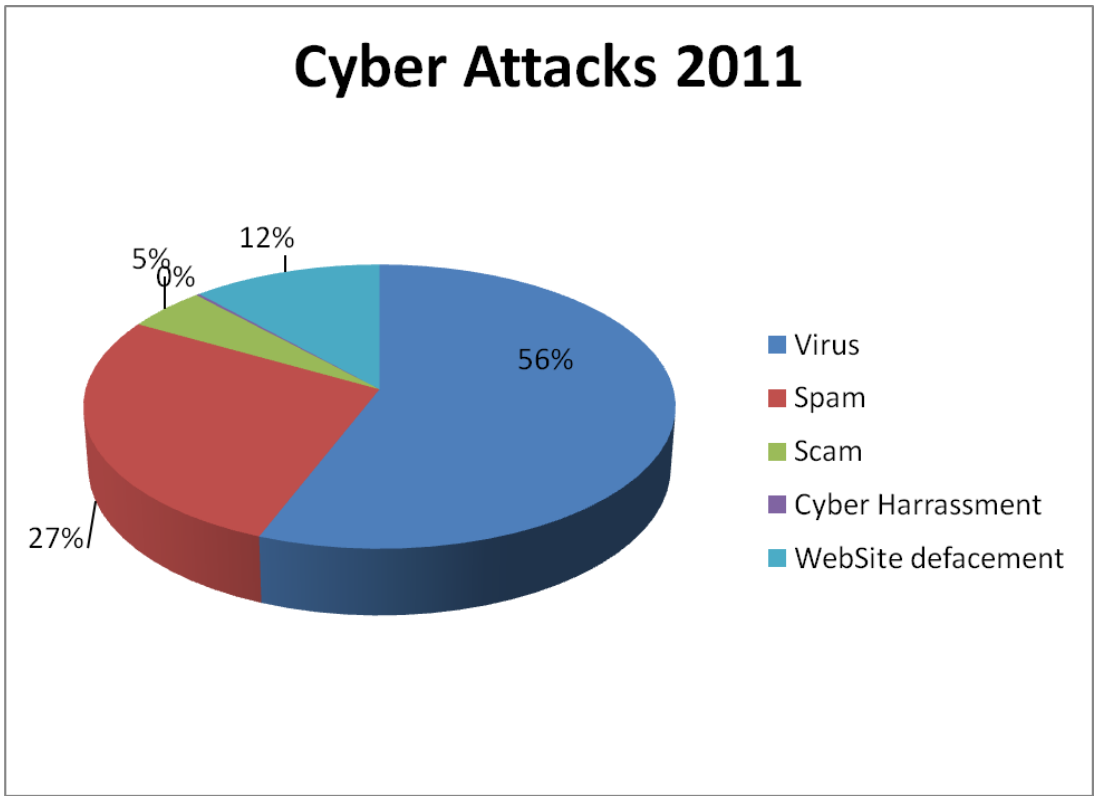


Figure 1

Types of Attack	Count
Virus	752
Spam	367
Scam	66
Cyber Harassment	3
Website Defacement	157

3.0 BruCERT Activities in 2011

3.1 Attended Seminars/Conferences/Meetings/Visits

BruCERT attended and presented at various seminars, conferences and meetings related to the field of ICT security.

- On 22nd March until 25th 2011 - Two BruCERT delegates attended the APCERT 2011 Annual General Meeting which takes place at Jeju Island South Korea.

- On 26th until 28th September 2011, BruCERT Attended the OIC-CERT Annual Conference 2011 and the 3rd Annual General Meeting.

- In February 22nd 2011, BruCERT joined the APCERT Drill.

- In September 27th 2011, BruCERT joined the ASEAN CERT Incident Response Drill, where the main objective is to simulate realistic cross-border incidents handling and promote collaboration among national CERTs in the region

3.2 Training and Seminars

From November 21st until November 25th, BruCERT hosted the OIC-CERT Technical Training which was conducted by MYCERT. It is the first time such an event had been organized in Brunei Darussalam. 13 countries participate in the incident handling training including some government agencies from Brunei Darussalam.

4.0 Conclusion

In 2011, BruCERT observed an improvement in IT security response in both the public and government agencies comparing to years before. Even though incidents reported to BruCERT are still far less comparing to other countries but this improvement gives a positive outcome where BruCERT will actively continue to improve its services as a national and government CERT. Hopefully with the ongoing and upcoming initiative such as BruCERT roadshows, security awareness to schools and publication of security awareness magazine will better educate the people the importance of IT security.

4. CERT-In Activity Report

Indian Computer Emergency Response Team - India

1.0 About CERT-In:

1.1 Introduction

CERT-In is a functional organisation of Department of Information Technology, Ministry of Communications and Information Technology, Government of India, with the objective of securing Indian cyber space. CERT-In provides Incident Prevention and Response services as well as Security Quality Management Services.

The Information Technology Act 2000 designated CERT-In to serve as the national agency to perform the following functions in the area of cyber security:

- Collection, analysis and dissemination of information on cyber incidents
- Forecast and alerts of cyber security incidents
- Emergency measures for handling cyber security incidents
- Coordination of cyber incident response activities
- Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents
- Such other functions relating to cyber security as may be prescribed

1.1.1 Establishment

CERT-In was operational since January 2004. The constituency of CERT-In is the Indian cyber community. CERT-In works cooperatively with Chief Information Officers and system administrators of various sectoral and organisational networks of its constituency.

1.1.2 Workforce power

CERT-In has 30 member technical staff.

1.1.3 Constituency

The constituency of CERT-In is the Indian cyber community and Indian cyberspace. CERT-In provides services to the organizations in the Govt., Public and Private sectors.

2.0 Activities and Operations of CERT-In

CERT-In provides:

- Proactive services in the nature of Advisories, Security Alerts, Vulnerability Notes, and Security Guidelines to help organisations secure their systems and networks
- Reactive services when security incidents occur so as to minimize damage

2.1 Incident handling Reports

The summary of activities carried out by CERT-In during the year 2011 is given in the following table:

Activities	Year 2011
Security Incidents handled	13301
Security Alerts issued	48
Advisories Published	81
Vulnerability Notes Published	188
Security Guidelines Published	4
White papers/Case Studies Published	3
Trainings Organized	26
Indian Website Defacements tracked	17306
Open Proxy Servers tracked	3294
Bot Infected Systems tracked	6277936

Table 1. CERT-In Activities during year 2011

2.2 Abuse Statistics

In the year 2011, CERT-In handled more than 13000 incidents. The types of incidents handled were mostly of Phishing, Malicious Code, Website compromise & propagation of malware and Network Scanning & Probing.

The year-wise summary of various types of incidents handled is given below:

Security Incidents	2004	2005	2006	2007	2008	2009	2010	2011
Phishing	3	101	339	392	604	374	508	674
Network Scanning / Probing	11	40	177	223	265	303	277	1748
Virus / Malicious Code	5	95	19	358	408	596	2817	2765
Spam	-	-	-	-	305	285	181	2480
Website Compromise & Malware Propagation	-	-	-	-	835	6548	6344	4394
Others	4	18	17	264	148	160	188	1240
Total	**23**	**254**	**552**	**1237**	**2565**	**8266**	**10315**	**13301**

Table 2. Year-wise summary of Security Incidents handled

Various types of incidents handled by CERT-In are given in Figure 1.

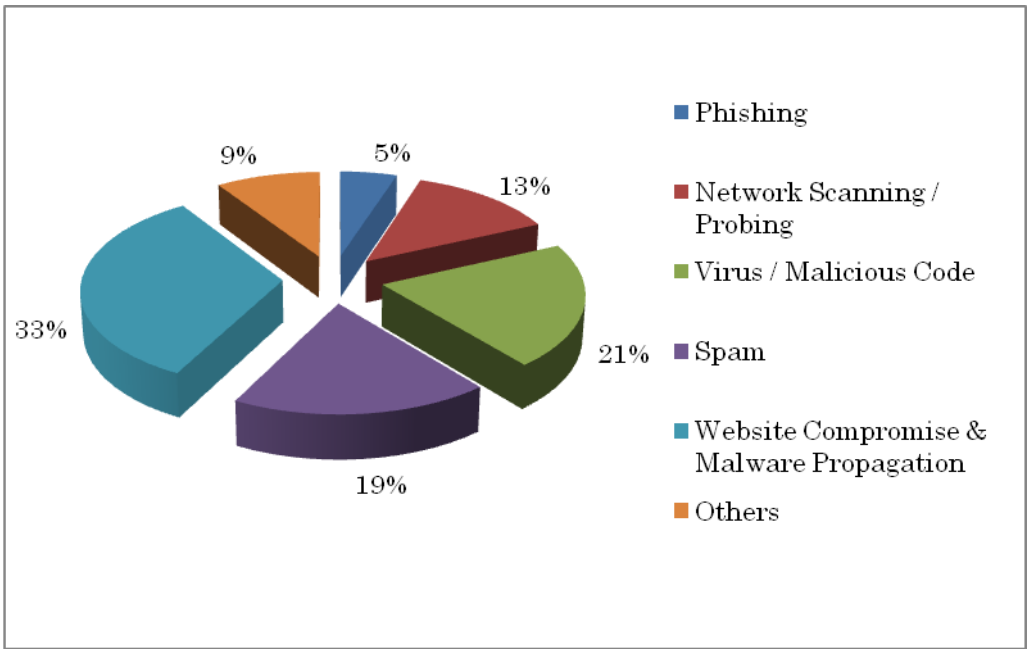


Figure 1. Summary of incidents handled by CERT-In during 2011

2.3 Incident Trends

The trends of incidents reported to and handled by CERT-In and cyber attack trends

during the year 2011 are as follows:

- Web site intrusions and drive-by-download attacks through compromised websites. Around 4394 malicious URLs were tracked in ".in" space. Most of the attacks were facilitated through attack tool kits such as Techno XPACK, Phoenix Exploit Kit, Neo spolit, Eleonre and Blackhole.
- Prominent client side vulnerabilities exploited in the drive by download attacks were in Adobe PDF, Flash, Java Runtime Environment, Interne Exporer and Mozilla Firefox.
- Malware trends indicate that malware affecting mobile platforms such as Android and Symbian were on the rise.
- Banking Trojans and key logger families were widely propagating. Prominent Trojans observed were ZeuS, Carberp, SpyEye, Torpig, Pushdo etc
- Rougue antivirus programs such as MacDefender, Winwebsec etc. were delivered to users through SEO poisoning
- Malicious Spam and identity theft schemes were leveraging Social networking sites and features therein
- Targeted attacks were on the rise involving exploitation vulnerabilities in Adobe PDF and MS Office.

2.4 Tracking of Indian Website Defacements

CERT-In has been tracking the defacements of Indian websites and suggesting suitable measures to harden the web servers to concerned organizations. In all 17306 numbers of defacements have been tracked. Most of the defacements were under .in domain, in which a total 9839 .in domain websites were defaced.

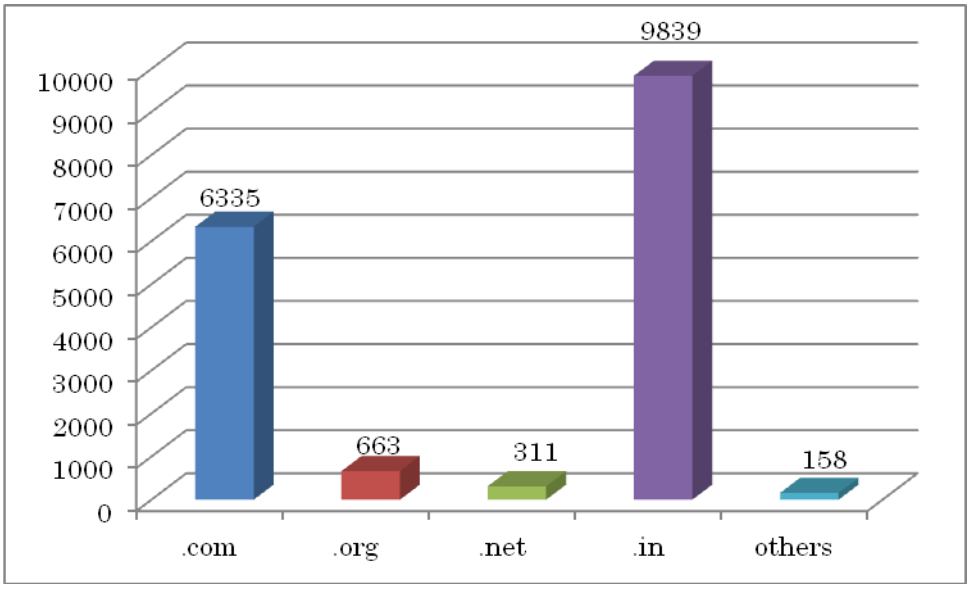


Figure 2. Indian websites defaced during 2011 (Top Level Domains)

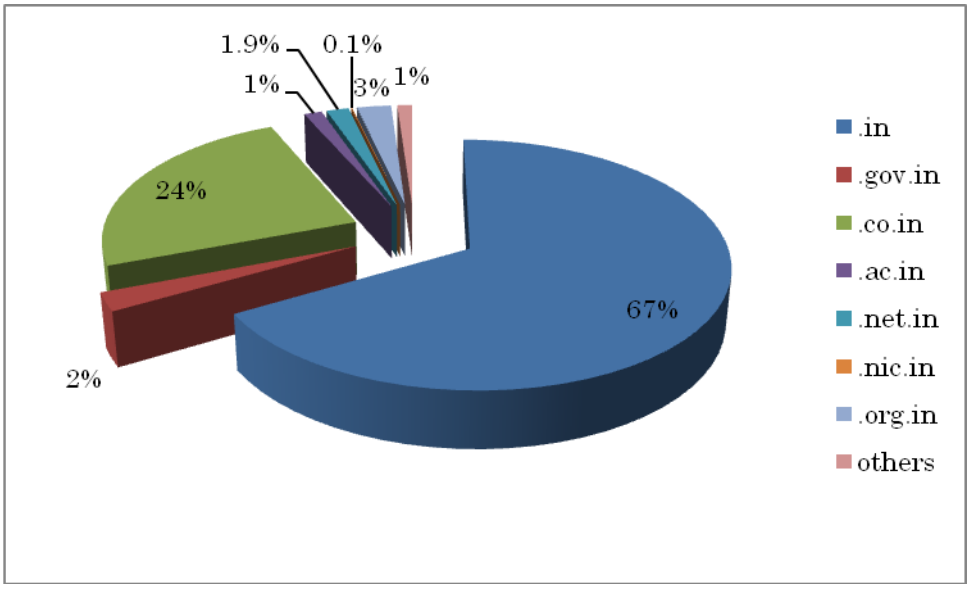


Figure 2.1 .in ccTLD defacements during 2011

2.5 Tracking of Open Proxy Servers

CERT-In is tracking the open proxy servers existing in India and proactively alerting concerned system administrators to properly configure the same in order to reduce spamming and other malicious activities originating from India. In all 3294 open proxy servers were tracked in the year 2011. The month-wise distribution of open proxy servers tracked during this year is shown in the figure 3.

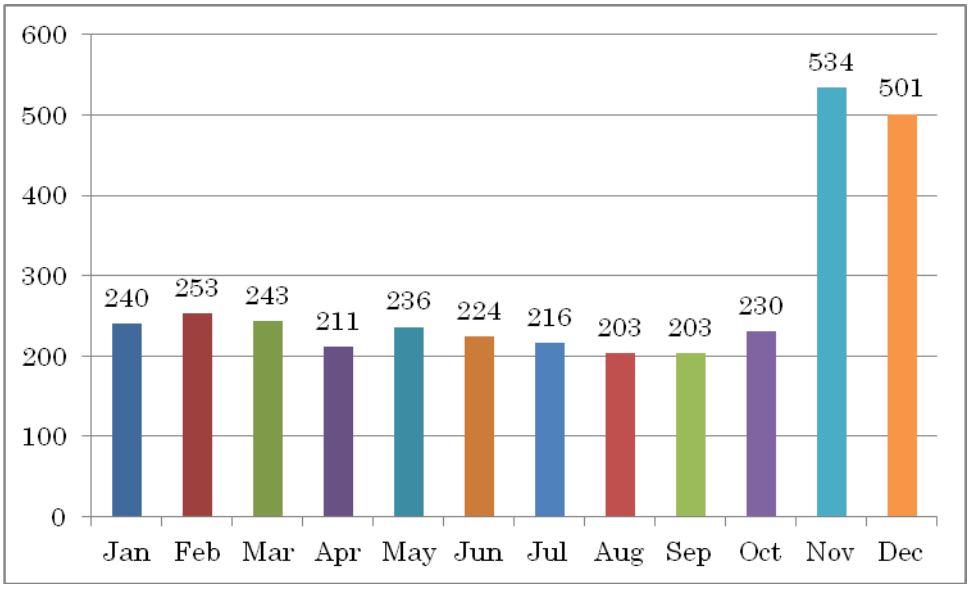


Figure 3. Monthly statistics of Open Proxy Servers in 2011

2.6 Botnet Tracking and Mitigation

CERT-In is tracking Bots and Botnets involving Indian systems. After tracking the IP addresses of Command and Control servers and Bots operating within India, actions are being taken to clean the respective systems and prevent malicious activities. Figure 4 shows the number of Bot infected systems and Command & Control servers tracked in 2011.

Month	Number of Bot Infected Systems	C&C Servers
January	2005349	11
February	1305033	21
March	1948356	32
April	2439756	33
May	2008282	45
June	2138201	7
July	2098347	7
August	2000925	9
September	2117432	7
October	2011193	4

November	2051836	2
December	1437170	3

Figure 4. Botnet statistics in 2011

2.7 Collaborative Incident resolution

During the year 2011, CERT-In worked in collaboration with Microsoft and Internet Service Providers in India to detect and clean the botnet infected systems, specifically the "Waldec" and "Rustock" Botnets. The outcome was very encouraging.

CERT-In also working in close coordination with cyber security agencies such as Symantec, McAfee and Kaspersky for resolution of incidents of malware such as Stuxnet and Duqu.

2.8 Interaction with Sectoral CERTs

CERT-In plays the role of mother CERT and is regularly interacting with the cyber security officers of Sectoral CERTs in Defense, Finance, Power, Transport and other sectors to advise them in the matters related to cyber security.

2.9 Security Profiling and Audit Services

CERT-In is providing Security Profiling and Audit services to key organizations within the country to identify risks, threats and vulnerabilities in their IT assets and advise appropriate mitigations.

3.0 Events organized/ co-organized

3.1 Education and Training

To create awareness and to enable users to implement best practices, CERT-In is organizing workshops and training programmes on focused topics for targeted audience such as CISOs, financial and banking sector officers, System Administrators, ISPs etc. Experts from industry are delivering lectures in these workshops apart from CERT-In staff. CERT-In has conducted the following training programmes during 2011.

- Workshop on "Secure Cloud Computing" on December 16, 2011
- Workshop on "Windows Security" on December 02, 2011

- Workshop on "Advanced Internet Investigations & Cyber Forensics" on November 18, 2011
- Workshop on "Secure Development Life Cycle" on November 15, 2011
- Workshop on "Targeted Attacks & Mitigation" on November 04, 2011
- Workshop on "Data Centre Security" on October 21, 2011
- Workshop on "Log Management, Compliance & Auditing" on October 17, 2011
- Workshop on "Phishing Attacks and Mitigation" on September 29, 2011
- Workshop on "Web Application Security : Current threats & mitigation" on September 09, 2011
- Workshop on "VoIP Security" on August 24, 2011
- Workshop on "Introduction to Web Application Security" on August 17, 2011
- Workshop on "Advanced Enterprise Security" on July 29, 2011
- Workshop on "Network Penetration Testing" on July 15, 2011
- Workshop on "Data Leakage Detection & Prevention" on June 24, 2011
- Workshop on "Advanced Web Application Security" on June 17, 2011
- Workshop on "Information Security Essentials" on June 10, 2011
- Workshop on "Virtualization Security Challenges" on May 27, 2011
- Workshop on "Advanced Cyber Forensics" on May 05, 2011
- Workshop on "Vulnerability Assessment in Enterprise Networks and Applications" on April 08, 2011
- Workshop on "Web Application Security - Current Trends" on March 18, 2011
- Workshop on "Linux Security" on March 11, 2011
- Workshop on "Network Perimeter Defence" on February 11, 2011
- Workshop on "MySQL Database Server Security" on February 04, 2011
- Workshop on "Introduction to Information Security" on January 28, 2011
- Workshop on "Oracle Server Security" on January 17, 2011
- Workshop on "SQL Server Security" on January 12, 2011

3.2 Drills

CERT-In has successfully participated in ASEAN CERTs Incident Handling Drill (ACID 2011) held in September 2011 and APCERT Incident Handling drill conducted

in February 2012.

At national level, CERT-In is carrying out mock drills with key sector organizations for assessing their preparedness in dealing with cyber crisis situation. These drills have helped in improving the cyber security posture of the information infrastructure and training of manpower to handle cyber security incidents, besides increasing the cyber security awareness among the key sector organizations. These drills at present are being carried out once in six months. Till date CERT-In has conducted 5 Cyber security drills of different complexities with 57 organizations covering various sectors of Indian economy i.e. Finance, Defence, Telecom/ISP, Transport, Power, Energy and IT industry.

4.0 Achievements

4.1 Publications

The following were published by CERT-In in the year 2011:

1. **Securing Wireless Access Points/Routers:** The purpose of the guideline is to recommend security practices for implementing Wi-Fi networks in Home and SOHO environments.
2. **Monthly security bulletins:** Monthly security bulletin comprises of Statistics of incidents handled by CERT-In, information on vulnerabilities in various Operating Systems and applications tracked, Cyber intrusion trends and other relevant IT security issues.

4.2 Certifications

Two technical members of CERT-In obtained GIAC Reverse Engineering Malware (GREM) Certification.

5.0 International collaboration

CERT-In has established collaborations with international security organisations and CERTs to facilitate exchange of information related to latest cyber security threats and international best practices. CERT-In is a member of Forum of Incident Response and Security Teams (FIRST), APCERT and Anti-Phishing Working Group (APWG).

5.1 MoU

CERT-In and US-CERT singed MoU to enhance cooperation in the area of cyber security for rapid resolution of and recovery from cyber attacks.

As part of MoU with National Computer Board, Mauritius, CERT-In is providing advice to make CERT, Mauritius fully operational and becoming member of Forum of Incident Response and Security Teams (FIRST).

6.0 Future Plans/Projects

6.1 Future projects

CERT-In has been evolved as the most trusted referral agency in the area of information security in the country. Following are the future plans:

- Regular interaction with CISOs of Critical Infrastructure Organisations and sectorial CERTs to ensure security of the critical systems.
- Development and implementation of a crisis management framework to enable organisations to respond to cyber incidents and assess the preparedness of organisations to withstand cyber attacks
- Enhancing collaborations with IT product and security vendors to mitigate the vulnerabilities in various systems and cooperation with international CERTs and security organizations on information sharing and incident response
- Promotion of R&D activities in the areas of attack detection & prevention, Cyber Forensics and malware detection & prevention.
- Creation of framework and facility for collection, correlation and analysis of security events in real time and generating early warning to constituency

5. CNCERT/CC Activity Report

National Computer network Emergency Response technical Team / Coordination Center of China – People's Republic of China

1. About CNCERT

1.1 Introduction

CNCERT (or CNCERT/CC) is a National level CERT organization under the leadership of MIIT (Ministry of Industry and Information Technology of the People's Republic of China). It serves as the national network security monitoring, early warning and emergency response center, as well as the key technical coordination organization concerning security issues in public network. Therefore, the vital roles it plays are as follows:

- Monitoring public network security,
- Collecting, analyzing and publishing network security threats,
- Notifying the communication industry of network security incidents,
- Receiving and handling network security incidents at home and overseas,
- Exchanging network security information and cooperating with international security organizations.

1.2 Establishment

CNCERT was founded in Sep., 1999, and became a member of FIRST in Aug 2002. It also took an active part in the establishment of APCERT as a founding member.

1.3 Workforce power

CNCERT, which is based in Beijing, the capital of P.R.China, has branch offices in 31 provinces, autonomous regions and municipalities of mainland China.

1.4 Constituency

The constituency of CNCERT includes the general public, government departments, the communication industry and the businesses in mainland China. It provides supports to the governmental departments for fulfilling their network security-related social management and public service functions, ensures the safe operation of national information infrastructure and undertakes the network security

monitoring, early warning and emergency response of control systems. Besides, it also assists the international internet organization to resolve network security incidents if the sources or targets are localized in mainland China.

1.5 Contact

E-mail：cncert@cert.org.cn

Hotline：+8610 82990999（Chinese）, 82991000（English）

Fax：+8610 82990375

PGP Key：http://www.cert.org.cn/cncert.asc

2. Activities & Operations

2.1 Incident handling reports

In 2011, CNCERT received 15,366 incidents reports[1] which increased by 47.3% from 10,433 in 2010. Most incident reports fell into the categories of vulnerability (36.3%), phishing (35.5%) and malware (23.4%) as shown in Figure 1.

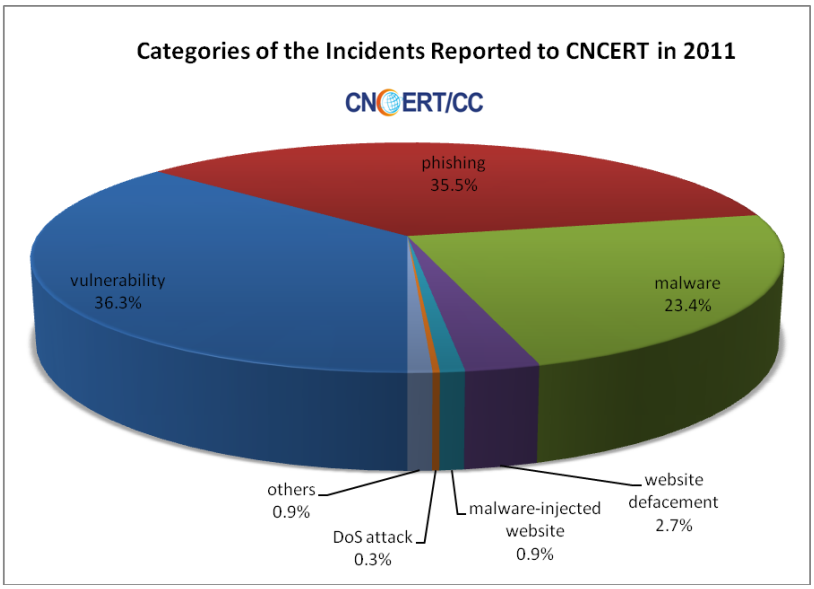


Figure 1 Categories of the Incidents Reported to CNCERT in 2011

[1]In 2011, CNCERT had not estimated spam incident reports in its data collection. Instead, suggested users turn to Anti-spam center of ISC for incident report.

In 2011, CNCERT handled 10,924 incidents, a rise of 2.4 times compared with that of the previous year. As shown in Figure 2, malware (46.6%) dominated the categories of the incidents handles by CNCERT in 2011, followed by phishing (34.2%) and website defacement (12.0%).

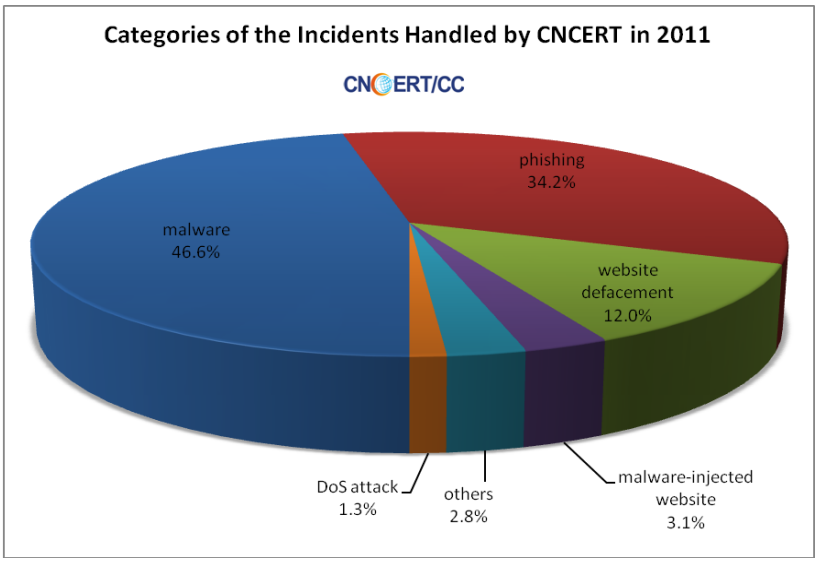


Figure 2 Categories of the Incidents Handled by CNCERT in 2011

2.2 Abuse Statistics

2.2.1 Trojan & Botnet Monitoring

According to CNCERT's sample monitoring, IPs of Trojan or Botnet C&C servers amounted to 300,407 in 2011, a reduction of 39.1% compared with that in 2010. As a result, 27,275,399 IPs of the hosts were infected with Trojan or Bot, which increased by 71.1% compared with that in 2010. About 46,723 IPs of Trojan C&C servers were identified as located outside of mainland China. The Top 3 affected countries or regions were Japan, the USA and Korea, as shown in Figure 3.

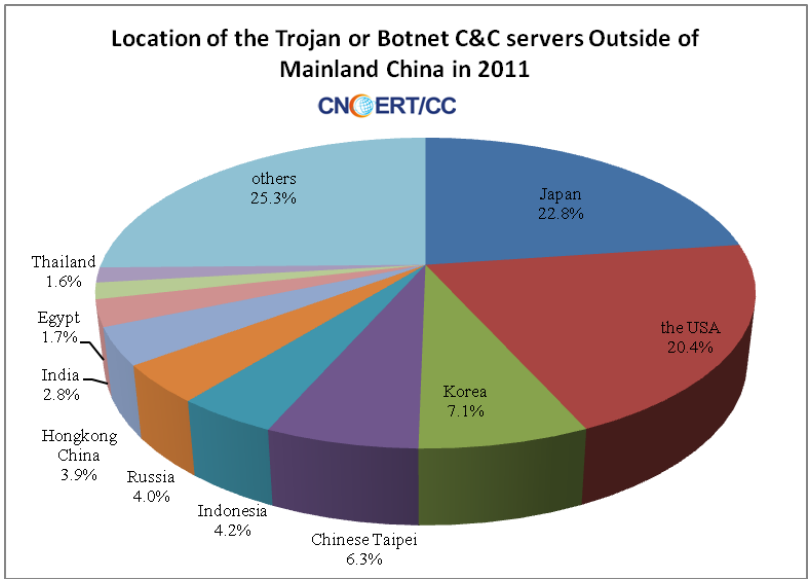


Figure 3 Location of the Trojan or Botnet C&C Servers Outside of Mainland China in 2010

2.2.2 Conficker Monitoring

Globally, there were over 35 million IPs of computer on average infected with Conficker each month. And China witnessed an average amount of 4 million IPs of computer fell victim to Conficker each month. As shown in Figure 4, the Top 5 affected disaster areas around the world were the USA (16.1%), mainland China (11.6%), Brazil (7.4%), Britain (3.8%) and India (3.2%).

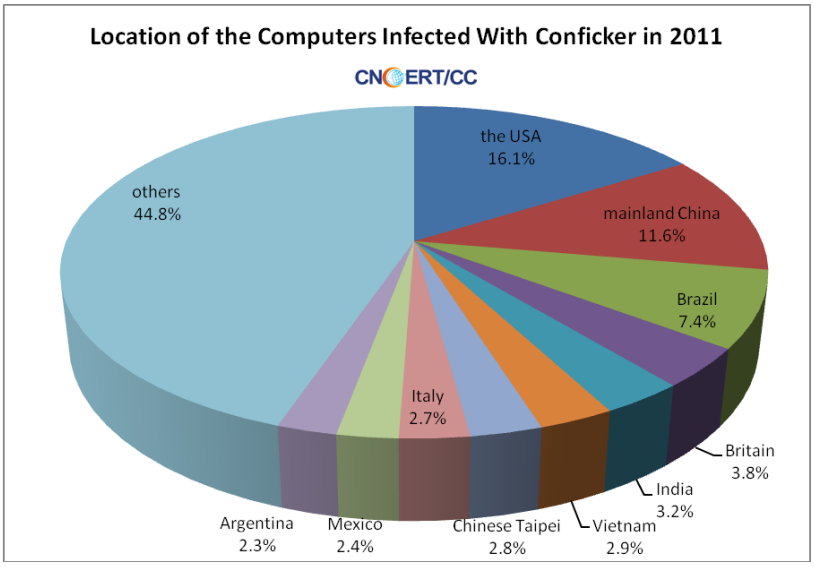


Figure 4 Location of the Computer Infected with Conficker in 2011

2.2.3 Malware Monitoring

In 2011, CNCERT monitored and discovered 35,821,698 malware incidents, which involved 785,388 malware download links, 67,468 malware-hosting domain names and 55,673 malware-hosting IPs. Figure 5 depicts the number of the malicious domains and IPs for spreading malware, with the most rampant activity after September. Meanwhile, port 80 (46.7%) and port 8080 (32.3%) were employed by the majority of the malware in the course of spreading.

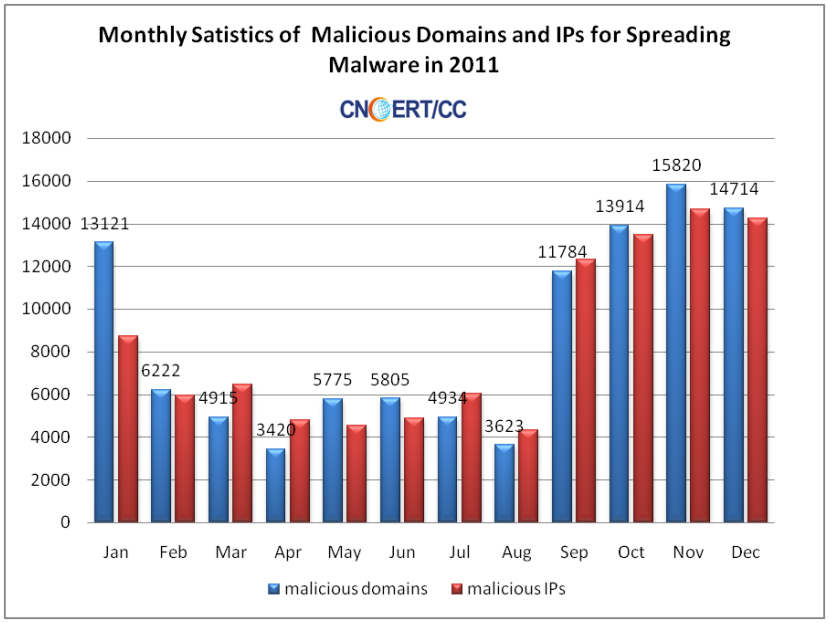


Figure 5 Monthly Statistics of Malicious Domains and IPs for Spreading Malware in 2011

2.2.4 Mobile Virus Monitoring

In 2011, CNCERT captured 6,249 mobile viruses in total. And an overwhelming amount still ran on the operation systems of Symbian (60.68%) and Android (39.3%). The malicious fee-deducting program topped the intention-based rank of the mobile malware with 1,317 (21.1%). Followed it were the ones intended for malicious propagation, stealing information, rogue action and remote control, accounting for 19.8, 18.9%, 18.5% and 17.6% respectively.

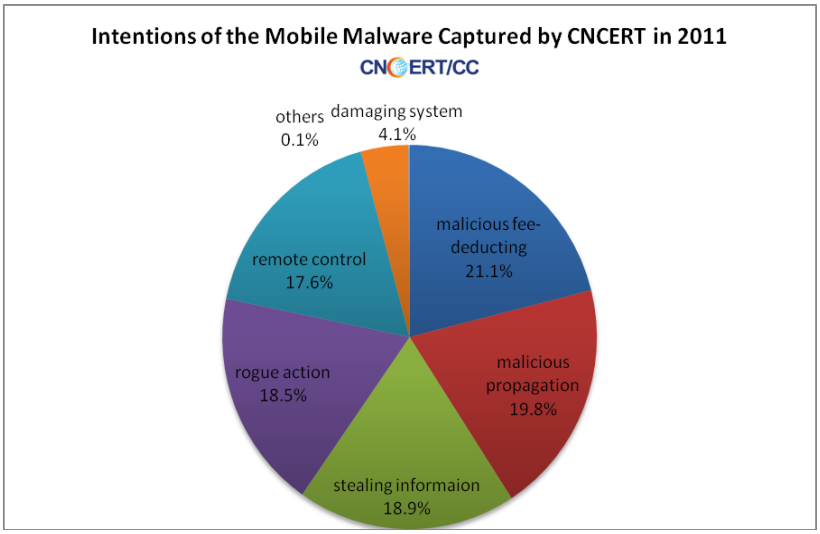


Figure 6 Intentions of the Mobile Malware Captured by CNCERT in 2011

2.2.5 Web Defacement Monitoring

According to CNCERT monitoring, 36,612 websites were defaced in mainland China in 2011, increasing by 5.1% from 34,845 in 2010. The defaced websites are categorized into .com & .com.cn, .gov.cn, .net & .net.cn, .org & .org.cn, .edu.cn and others based on their domains. As shown in Figure 7, .com & .com.cn still dominated the domain categories of the defaced website, while .gov.cn accounted for 9.6% with a considerable decrease of 39.4% in 2011.

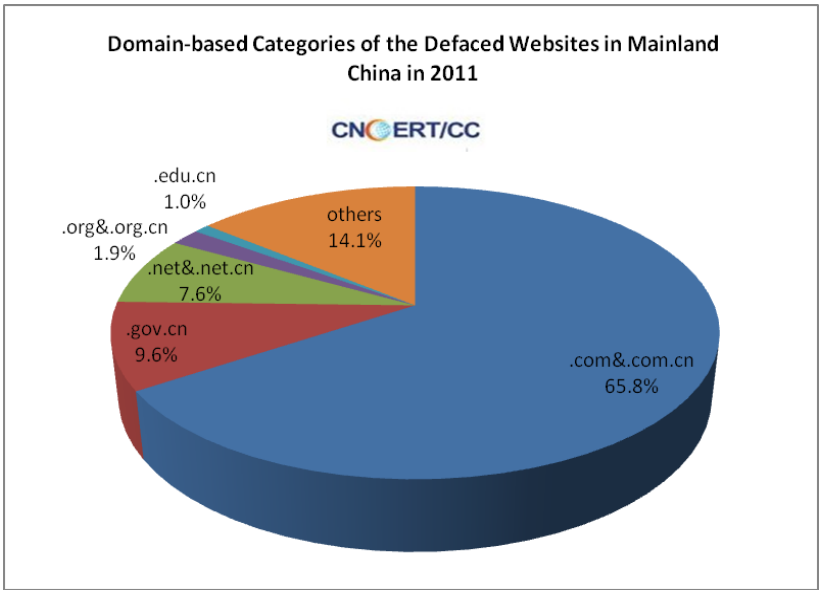


Figure 7 Domain-based Categories of the Defaced Website in Mainland China in 2011

2.2.6 Phishing monitoring

From March to December in 2011, CNCERT monitored 3,841 domains of phishing websites masquerading as legitimate banks in mainland China, which were resolved to 667 IP addresses home and abroad. Figure 8 illustrates location of the phishing servers' IPs, 72% of which were identified as in the USA.

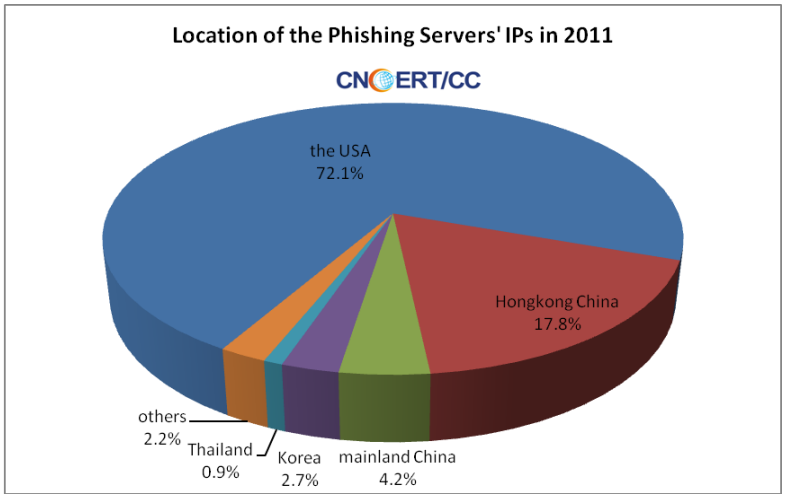


Figure 8 Location of the Phishing Servers IPs in 2011

2.2.7 Backdoor monitoring

From April to December in 2011, CNCERT monitored 12,513 websites injected with backdoor in mainland China, including 1,167 government sites (.gov.cn). There were 11,851 source IPs of the attacks located outside of mainland China, mainly in the USA, Korea, Nigeria and Turkey.

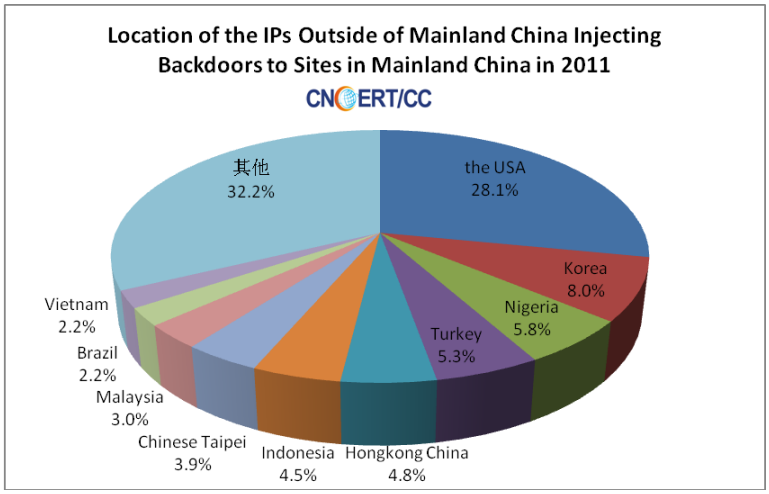


Figure 9 Location of the IPs Outside of Mainland China Injecting Backdoor to Sites in Mainland China in 2011

3. Events organized/co-organized

3.1 Drills

CNCERT participated in three drills in 2011 to exercise incident response capacity and to mitigate the impact of ongoing internet attacks, enabling better coordination with local and international partners. These drills are as follows:

APCERT 2011 Drill-"Critical Infrastructure Protection", on Feb. 23, 2011

MIIT (Ministry of Industry and Information Technology) 2011 Drill, on Jun. 7, 2011

ASEAN CERT Incident Drill (ACID) 2011, on Sep. 27, 2011

3.2 Conferences

Press Briefing of Report on 2010 Network Security Landscape

CNCERT co-hosted this briefing with the Communication Security Bureau of MIIT on March 9 in Beijing. The report analyzed the network security in 2010 and predicated security trend in the coming year with some countermeasures suggested.

2011 CNCERT Annual Conference

CNCERT hosted this conference from August 8 to 10 in 2011 at Dalian city, China in the theme of 'New Perspectives New Security'. The mission was presenting and sharing new emerging focus and concerns on network security, and discussing new countermeasures or approaches to deal with them.

4th China-ASEAN Network Security Seminar

CNCERT organized the 4th China-ASEAN Network Security Seminar in Dalian, China on August 8, 2011. The seminar offered an opportunity for the CNCERT and ASEAN delegates to exchange network security technology and management experience and to strengthen bilateral cooperation mechanisms.

Symposium on "Fighting Spam to Build Trust"

CNCERT co-chaired this symposium with Messaging Anti-Abuse Working

Group (MAAWG) at the EWI's Second Cybersecurity Summit, which was held on June 1 to 2 in London. The participants discussed how to set up the international anti-spam forum and to implement the best practices.

4. Achievements

4.1 Publication

Figure 12 lists publications of CNCERT throughout the year 2011.

Name	Issues	Description
Weekly Report of CNCERT (Chinese)	52	Emailed to over 430 organizations and individuals and published on CNCERT's website (http://www.cert.org.cn/)
Weekly Report of CNCERT (English)	18	Emailed to over 430 organizations and individuals and published on the English page of CNCERT's website (http://www.cert.org.cn/english_web/documents.htm)
CNCERT Monthly Reports on Internet Security Threats (Chinese)	11	Issued to over 400 organizations and individuals on regular basis and published on CNCERT's website (http://www.cert.org.cn/)
Annual Report on Network Security (Chinese)	1	Published on CNCERT's website (http://www.cert.org.cn/)
CNVD Vulnerability Weekly Report (Chinese)	52	published on CNCERT's website (http://www.cert.org.cn/)
Network Security Alerts (Chinese)	41	published on CNCERT's website (http://www.cert.org.cn/)
Fighting Spam to Build Trust (Chinese and English)	1	http://www.cert.org.cn/articles/activities/common/2011081625464.shtml http://www.ewi.info/fighting-spam-

		build-trust

5. Conferences attended & speeches delivered

APCERT Annual Conference and Annual General Meeting

This conference was held from March 22 to 25 at Jeju, Korea. In the conference, China delivered the speech on the network security status in China, initiated and chaired the information sharing workgroup and actively joined discussions to promote the role of CNCERT in international mutual and multi-lateral cooperation.

43rd and 44th Meetings of the APEC Telecommunications and Information Working Group (TEL)

The 43rd and 44th Meetings of the APEC TEL were held in March and September respectively. CNCERT attended the workgroup session especially on network security.

23th Annual FIRST Conference and 2011 Annual Meeting for CSIRTs with National Responsibility

These two conferences were held in Vienna, Austria from June 6 to 12. CNCERT delivered a keynote speech on technical requirements for national-level CSIRT as well as potential challenges and development directions in future, which were well recognized by the participants.

6th China-ASEAN Telecom Round Table Seminar

This seminar was held in Brunei on July 14, 2011. CNCERT expressed the wishes of pushing forward cooperation in the field of regional network security together and ushering prosperity in information and telecommunication.

6. HKCERT Activity Report

Hong Kong Computer Emergency Response Team Coordination Centre - Hong Kong, China

1. About HKCERT

1.1 Establishment

Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) was established in 2001 with funding from the Hong Kong Special Administrative Region (HKSAR) Government. The Hong Kong Productivity Council (HKPC), which is a government subvented organization in Hong Kong, has operated the centre since then.

1.2 Mission and Constituency

HKCERT is the centre of coordination of computer security incident response for local enterprises and Internet users in Hong Kong. Her missions are to handle computer security incident reports, gather and disseminate information relating to security issues, advise on preventive measures against security threats, promote information security awareness, and maintain network with other computer emergency response teams (CERT) and security organizations to facilitate coordination and collaboration.

1.3 Organization

The senior management of HKPC oversees the overall direction and operation of the centre. The daily operations are taken care by the Centre Manager, two consultants and a group of computer security specialists.

2. Operations and Activities

2.1 Incident Handling

HKCERT serves as a coordination centre for information security incidents of Hong Kong. HKCERT is recognized as the national CERT for the economy of Hong Kong and the point of contact in cross border information security incidents.

During the period from January to December of 2011, HKCERT had handled 975 incidents, including 810 security incidents, 145 virus incidents and 20 other incidents. Security incident reports continue to overtake virus incident reports (See Figure 1).

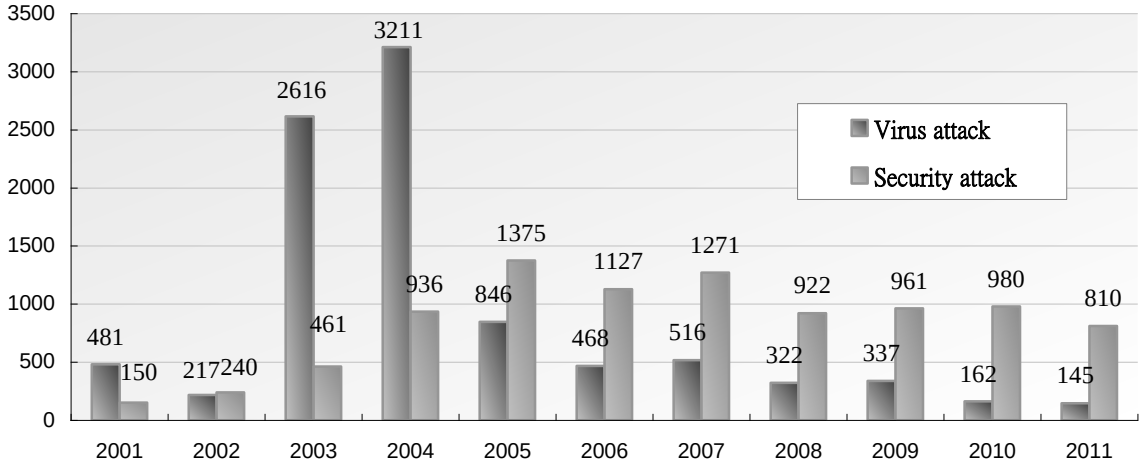


Figure 1. HKCERT Incident Reports in 2011

The number of incidents reported by local parties was 400 (34.3%), by overseas parties was 405 (34.7%) and by proactive discovery was 360 (30.9%).

Source locality of reports	2010	2011
Local parties	360 (26.3%)	400 (34.3%)
Overseas parties	554 (40.6%)	405 (34.7%)
Proactive discovery	452 (33.1%)	360 (30.9%)

- The continuing low local reports indicated that malware nowadays are more stealth than before. We have to do more awareness promotion to educate the general public about the threats.
- The significant number of cross border incidents reflected the globalization of cyber attacks and a need for building strong international collaboration.
- We have to conduct proactively research to effectively discover previous unreported incidents.

Proactively discovered incident reports are a result of discovery research conducted by HKCERT staff. Defacement websites and phishing sites were among the top 3 in 2010 and 2011. In 2011, malware infection climbed up to second and code injection (9.2%) went to the fourth place,

Top 3 incident types via Proactive Discovery	2010	2011
1	Defacement (33.4%)	Defacement (33.9%)
2	Phishing (31.6%)	Malware (25.8%)
3	Code Injection (14.8%)	Phishing (23.9.9%)

2.2 Information Gathering and Dissemination

HKCERT collected security-related information from security organizations, made judgments on the impact to Hong Kong, and decided whether to disseminate the information. During the period from January to December of 2011, HKCERT published 343 security bulletins and advisories (See Figure 2) which is an 11% increase from previous year's number (i.e. 308). All security bulletins were related to vulnerabilities and no malware alert was published during this period.

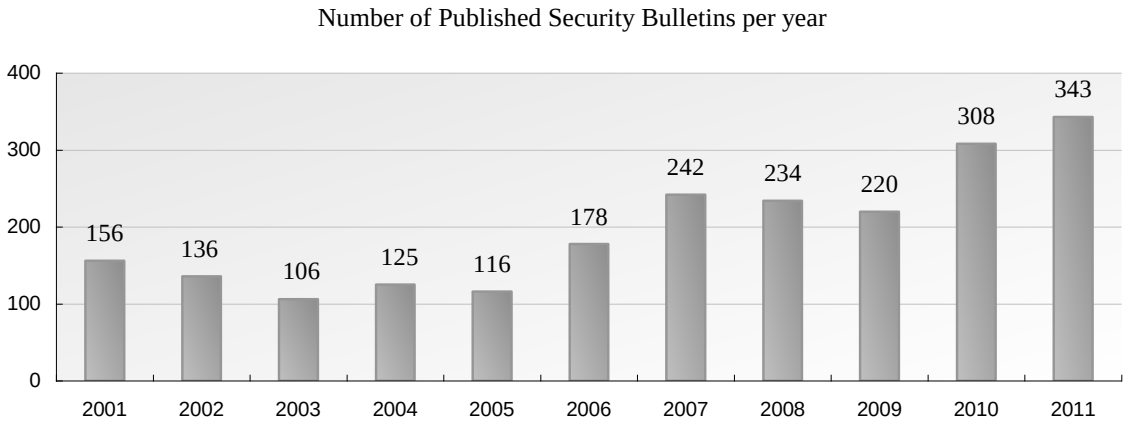


Figure 2. HKCERT Published Security Bulletins in 2011

2.3 Publications

We had published 12 issues of monthly e-Newsletter in the period.

The **Information Express RSS feed services** continued to be well received. There were 1,182,911 RSS visitors in 2011, representing **a 104% increment compared with the previous year**.

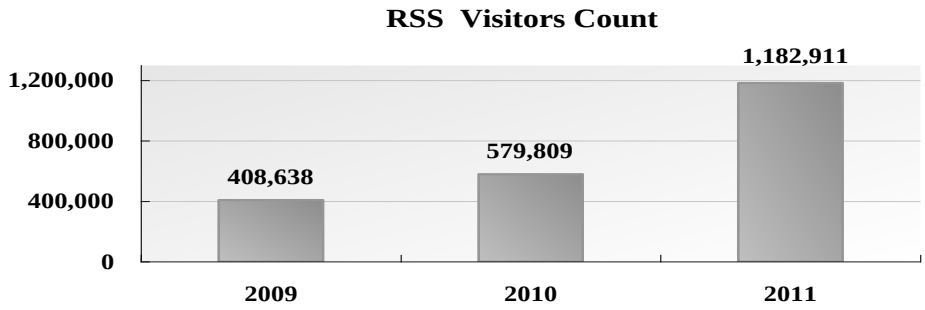


Figure 3. HKCERT RSS Visitors Count in 2011

3. Security Awareness and Training

3.1 Seminars, Conference and Meetings

HKCERT jointly organized the Hong Kong Clean PC Day 2011 campaign with the Government and Police. The campaign involved public seminars, cyber security symposium and a screensaver contest. Five public seminars were organized in March, June, August, October and December 2011.

We organized the Information Security Summit 2011 with other organizations and associations in November 2011, inviting local and international speakers to provide insights and updates to local corporate users.

3.2 Training

We coordinated two overseas expert and two local experts to deliver three speeches and three hands-on workshop on "Analysis and Reverse Engineering Android Malware", "Deploying a Secure Private Cloud" and "Penetration Test Kungfu with BackTrack" in the training workshops of the Information Security Summit.

3.3 Speeches and Presentations

HKCERT was invited to deliver speeches and presentations on various occasions for Government, associations and schools.

3.4 Media briefings and responses

HKCERT was interviewed by the media from time to time to give objective and professional views on information security topics and incidents.

4. Coordination and collaboration

4.1 International Collaboration

HKCERT participated in a number of international coordination and collaboration events:

4.1.1 Collaboration with CERT community

- Served in the APCERT Steering Committee in 2010-2012; elected as the Chair for 2010-2011
- Participated in APCERT AGM and Conference 2011 in Jeju, Korea (March 2011)
- Participated in both the FIRST AGM and Conference 2011, organized by FIRST, and the Annual Meeting for CSIRTs with National Responsibility, organized by CERT/CC in Vienna, Austria (June 2011)
- Participated in the APCERT Drill (Feb 2011) and also acted was the Exercise Control team member. The theme of the drill this year was "Critical Infrastructure Protection". The drill was a great success with 20 APCERT from 17 economies participating.
- Joined the Tsubame distributed honeypot project of JPCERT/CC
- Liaised with Macao CERT (MOCERT) in her application to APCERT and FIRST and paid a site visit to MOCERT (May 2011)

4.1.2 Collaboration with other international organizations

- Represented APCERT in the Advisory Council of DotAsia Organization
- Joined the Microsoft Security Cooperation Program to share information
- Participated in Digital Crime Consortium Conference in the Bahama Islands, organized by Microsoft (Oct 2011)
- Participated in Honeynet Project Workshop 2011 in Paris (March 2011)
- Participated in the AVAR Conference in Hong Kong (Nov 2011)

4.2 Local Collaboration

HKCERT worked with a number of local organizations in different areas:

- Continued to work closely with the government and law enforcement agency, and held meetings to exchange information and to organize joint events regularly
- Continued to work with police, ISPs and domain registries on closing down bulletproof hosting, phishing sites and botnet command and control centres in Hong Kong. HKCERT is still working closely with HKIRC on pre-empting the risks caused by Conficker worm generating pseudo-random domains with ".hk".
- Co-organized a local drill with HK Police and OGCIO on 4th November 2011 on web forum incident response. HKCERT led the preparation of the scenarios and acted as the lead of EXCON of the drill. The drill was a great success.
- Participated in the government's Information Infrastructure Liaison Group and Information Security Task Force and provided security status reporting during World IPv6 Day, and important events such as the policy address of CE and the budget speech
- Maintained the Information Security Advisory and Collaboration (ISAC) Mailing list and advised on latest information security issues through the list
- Organized a round table discussion meeting with information security organizations

5. Other Activities

5.1 Year Ender press briefing

HKCERT organizes a year ender press briefing to media at the beginning of each year, to report on information security status in the past year, and to give perspective of the trends of security attacks in the coming year to warn the public for better awareness and preparedness.

The 2011 year ender briefing was held on 4th January 2012.

5.2 Website revamp

HKCERT revamped the website and launched it officially in 2011. The website supports mobile device and has social network feature. The security of the HKCERT

website was enhanced by adopting SSL protection for all pages. In the new website, security bulletins would be given severity rating to help users to prioritize their mitigation measures.

6. Future Plans

6.1 Funding

HKCERT would secure Government funding to provide the basic CERT services in 2012/2013. We shall work closely with the government to plan for the future services of HKCERT.

We shall continue to propose new initiatives to the government and seek support from the government.

6.2 Enhancement Areas

**HKCERT had conducted a strategic review of services by JPCERT/CC in late 2009. The review had pointed out areas for improvement which we are working on thean strategic plan to incorporate implementation plan on these recommendations in future plan and seek funding to support them. They include enhancement of incident management system, proactive discovery of security incidents, intelligence collection,

From the incident report statistics we found that strengthening proactive discovery could probably generate good results. We plan to invest more resources to allow tracking of more information sources and automation the process. mobile security incident handling and malware analysis capability.

7. ID-CERT Activity Report

Indonesia Computer Emergency Response Team - Indonesia

1. About ID-CERT

1.1 Introduction

ID-CERT (Indonesia Computer Emergency Response Team) is an independent team which is from and for community. ID-CERT is the first CERT in Indonesia and founded by DR. Budi Rahardjo in 1998. ID-CERT together with JP-CERT (Japan), AusCERT (Australia) is one of the founders of the APCERT (Asia Pacific Computer Emergency Response Team) forum.

1.2. Establishment

In 1998 there was no CERT in Indonesia. Based on that DR. Budi Rahardjo, an internet security expert, encouraged himself to establish ID-CERT. At the same time countries around Indonesia began to establish their own CERTs and this continued into Asia-Pacific forum which later became the APCERT.

ID-CERT wishes to remain standing as a non-governmental organization, independent, but received an allocation of government funding as a contribution to the CERT. ID-CERT is just being reactive (not active) in responding and handling a case of incoming or reported incident by complainers. ID-CERT does not have the authority to investigate a case thoroughly, but just become a liaison who can be trusted, especially by those who reported incident.

1.3 Workforce power

During 2011 complaints received by ID-CERT were still handled by Dr. Budi Rahardjo and Andika Triwidada. Since January, 2011 Ahmad Alkazimy was recruited after being volunteer in research activity since March, 2007.

1.4 Constituency & Etc.

At the end of 2011, ID-CERT had successfully expanded its constituencies to ISP, NAP, Government bodies, ccTLD-ID Registry, Corporates, Professional Associations and individuals.

In addition, ID-CERT also had succeeded in formulating its mission together with the community and its constituents. The missions are:

1. ID-CERT's purpose is to coordinate the incidents handling involving community locally and internationally.
2. ID-CERT does not have operational authority to its constituency, it only informs a variety of complaints to network incidents, and depends entirely on the cooperation with all those involved in incidents related networks.
3. ID-CERT is built from community and the results will be given back to the community.
4. ID-CERT helps increasing the internet security awareness in Indonesia.
5. ID-CERT has research in internet security which is needed by the Indonesia internet community.

2. Activities and Operations

2.1. Activities

2.1.1 Incident Handling Reports

Abuse category consists of:

Spam	Spam complaints received from abroad to the network in Indonesia
Spam Complaint	Spam complaints received from domestic/local to the network in Indonesia and abroad
Response	The response provided by all parties on incoming reports
Network Incident	Activities carried out on other people's networks as well as all activities related to network abuse
Fraud	Report misuse of credit cards. This definition is based on reports police/law enforcement
Spoofing / Phishing	E-mail scams and websites to deceive users
Malware	A computer program created with malicious intent

IPR	Intellectual Property Rights

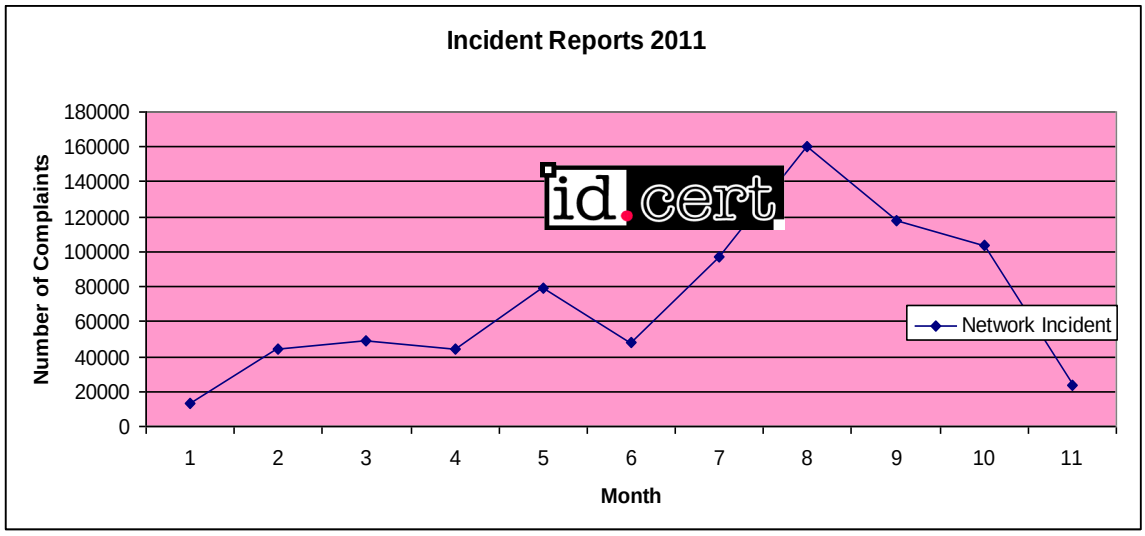


Figure 1: Incident Handling Reports 2011

Most of the complaints that ID-CERT received on 2011 from the communities were Network Incident.

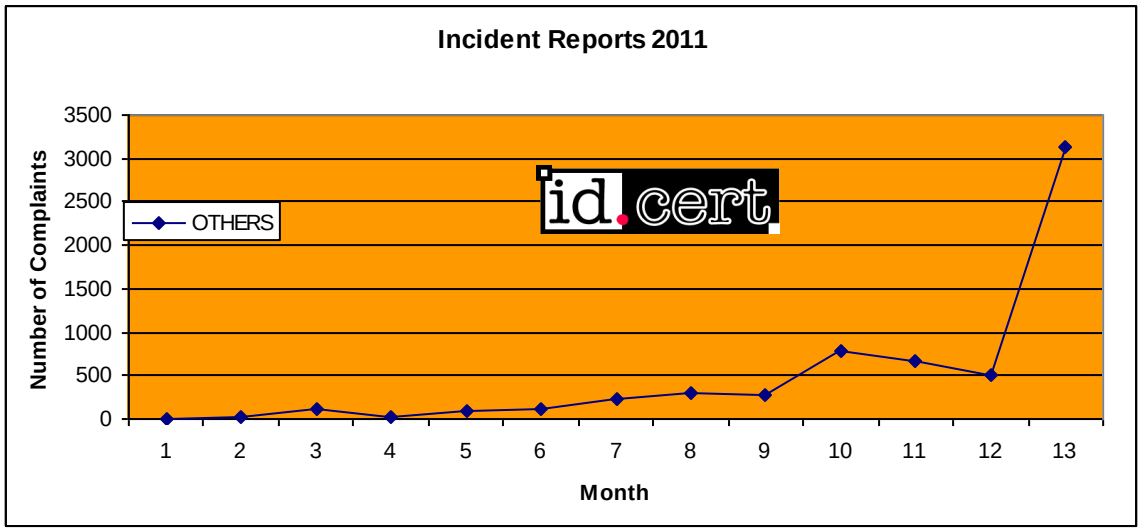


Figure 2: Incident Handling Reports 2011

Other complaints that ID-CERT received were: Malware, Spoofing/Phishing, Spam, Spam Complaints and Response.

2.1.2 Research on Indonesia Internet Abuse 2011

The research initiated several years ago in creating Internet Security statistics based on reports received by ID-CERT only.

In 2011 ID-CERT added more respondents to get more data besides the current one from ID-CERT. Totally 45 respondents had joined the Internet Abuse research by the end of 2011, including ID-CERT, PANDI (ccTLD-ID Registry), 3 Ministry Offices, 5 telecommunication operators, 7 NAPs, 25 ISPs, and 2 foreign respondents. The type of data ID-CERT got from the respondents were Summaries of Abuse reports received by each respondent or email copies of Abuse reports received by each respondent.

In contrast to reports received by the ID-CERT itself, the amount of average consolidated complaint received through Internet Abuse Research in 2011 amounted to 26,095 reports.

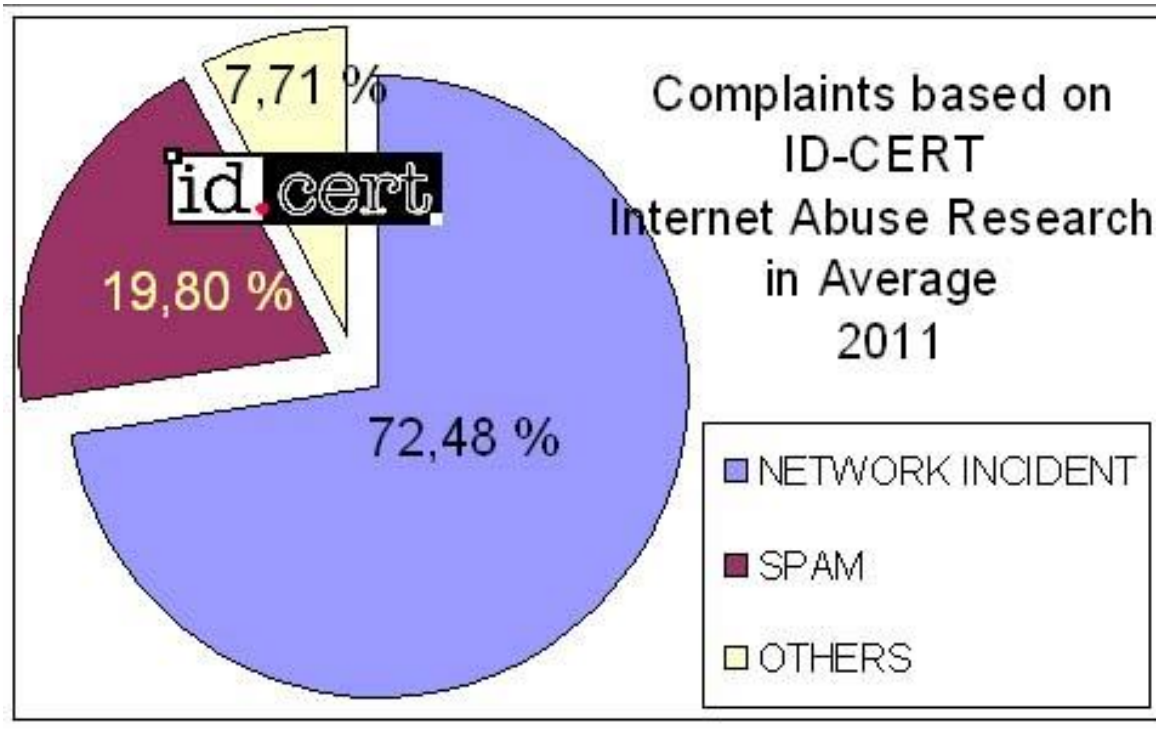


Figure 2: Research on Indonesia Internet Abuse Statistics 2011 (Monthly average, in %)

Figures shown above were the average abuse complaints ID-CERT received from the

43 local and 2 foreign respondents. The biggest level was the network incident, followed by the second large complaints were the spam.

2.2. Operations

E-mail abuse@cert.or.id was activated in January 1, 2011 to receive data from Research on Internet Abuse respondents.

E-mail cert@cert.or.id was also created to receive complaints.

ID-CERT plans to create some complaint e-mails which clasified based on most reports received.

3. Events

In February 28, 2011 ID-CERT had its third Public Gathering in Jakarta. A number of topics were discussed in the gathering, they are:

1. Current and future services
2. Abuse Research update
3. Funding
4. Formalizing ID-CERT Framework based on RFC2350.

In March 22-25, 2011, the APCERT AGM was held in Jeju, South Korea. ID-CERT could attend it after absent for several years. Thanks to APCERT and KrCERT for facilitating it.

4. Collaboration

4.1 Local

In July 2011 the first meeting between ID-CERT and APJII continued to have an MoU in November 2011.

ID-CERT also added its service by providing feed report to KAMINFO (Directorate of Information Security, Ministry of Communication and Information) regarding to government sites which got defacing/phishing.

ID-CERT was invited several times by KAMINFO in some events, such as Workshop of Handling Information Security Incident and Indonesia Internet Security Forum (IISF), and as a keynote speaker in CERT Regulation meeting.

4.2 International

ID-CERT got email feed from some foreign organizations for all IP address and domain names related to Indonesia. Some foreigner CSIRTs from Europe to Latin America (including GovCERT and Financial CERT) often make coordination with and asking help from ID-CERT.

5. Future Plan

ID-CERT has a number of plans related to future development of ID-CERT.

First thing to do, ID-CERT will employ several full-time staffs to increase incident handling capacity. A response help desk officer will be recruited soon. ID-CERT will also plan to send its staff for an internship to another CERT. It means that the employee of ID-CERT could have a complete picture of CERT services in general.

Second one, ID-CERT will deploy a system to manage and handle incidents better. ID-CERT will prepare the workflow and Standard Operation Procedures (SOP).

In addition, research activities, such as Abuse Research, a local product of ID-CERT for the needs of their constituents, will continue to work on. ID-CERT plans to maintain the data until the next few years.

ID-CERT will prepare several other researches and studies, required by Indonesia internet community. ID-CERT also plans to add personnel in the field of research and collaboration with leading universities in developing any necessary research.

ID-CERT will publish regular research reports per month, per bi-monthly, per semester, and annual report.

The last, the most ID-CERT's attention is: what exactly will be expected by society from ID-CERT.

6. Contact Information

Web : http://www.cert.or.id
E-mail : cert@cert.or.id (incident complaint)
abuse@cert.or.id (Internet Abuse Research)
Phone : +62 838 74 9292 15 (Mr. Ahmad Alkazimy)

PGP Keys :
Mr. Andika Triwidada
E-mail: andika@cert.or.id
Fingerprint=5568 7C7D E898 4F33 A594 A996 DA4B C29F E22D FEE7

Mr. Ahmad Alkazimy
E-mail: ahmad@cert.or.id
Fingerprint=39B2 87BA 3DD6 7832 D56F 0344 FCE4 3A7C FE38 CC96

7. Conclusion

After facing the hard times, ID-CERT attempted to rise again as a community-based CERT.

As for the future based on ID-CERT's views: in Indonesia, will appear more sectors CERT such as banking CERT, government CERT, education CERT, etc based on the need of their own community to coordinating to each other.

In the year 2011, though only a few abuse reports that come in, ID-CERT planned to continue enhancing the ability of ID-CERT personnel through training and plan for internship.

Another issue that ID-CERT found last year was the difficulty to contact the content provider/social networking providers such as Facebook, Twitter, Yahoo and Google. Finally, the issues had been resolved. Thanks to APCERT team.

8. Id-SIRTII/CC Activity Report

Indonesia Security Incident Response Team on Internet Infrastructure - Indonesia

1. About Id-SIRTII/CC

1.1 Introduction

Id-SIRTII/CC is the national CSIRT/CC of Indonesia. The purpose of Id-SIRTII is to coordinate security efforts and incident response for critical infrastructure and IT-security problems on a national level in Indonesia.

1.2 Establishment

Id-SIRTII/CC was established in 2006 by ICT Minister Decree Number 27/2006 and 26/2007 then revised with 16/2010. On 2010 became a full member of APCERT. On 2011 became a member of FIRST and also National CSIRT Forum. On 2009 became a member of OIC-CERT.

1.3 Workforce Power

Id-SIRTII/CC now has 6-team member, which is Chairman and 5 deputy (Vice Chairman). For supporting daily operations we employ 35 staffs in our office at Jakarta the Capital City of Indonesia.

1.4 Constituency etc.

Our constituencies are:

- IT security teams (public sectors)
- Internet Service Provider (ISP)
- Network Access Provider (NAP)
- Local Internet Exchange Operator
- Law Enforcement Agency (LEA)
- Critical Infrastructure Operators
- Other Sectors CSIRT's in Indonesia.

Our main activities are:

- Socializing to related parties to conduct security activities of the telecommunications network utilization of IP-based

- Monitoring, detection and early warning of threats and disturbance of the telecommunications network of IP-based in Indonesia
- Developing and / or providing, operating, maintaining and developing the database system of monitoring and conducting security activities of the telecommunications network utilization of IP-based at least for monitoring, early detection and early warning of threats and disturbance to the telecommunications network utilization of IP-based, keeping records of transactions (log files) for supporting the law enforcement process
- Performing the functions of information services to the threats and security disturbance of the telecommunications network utilization of IP-based
- Carrying out research and development activities, providing simulation lab and training activities of the telecommunications network utilization security of IP-based
- Providing consultancy services and technical assistance to strategic institutions/agencies
- As a central coordination (Coordination Center / CC) and liaison (Single Point of Contact) with related agencies /institutions both in the country and abroad.

2. Activities and Operation

2.1 Incident Reports

There is no direct incident report yet. We will provide Incident Reporting Service for public in the first quarter of year 2012. We only authorized to address all types of computer security incidents, which occur, or threaten may occur in our Constituency and which require cross-organizational coordination. The level of support given will vary depending on the type and severity of the incident or issue, the type of constituent, the size of the user community affected, and the availability of Id-SIRTII`s resources at the time. Special attention will be give to issues affecting critical infrastructure. No direct support will be given to end users they are expected to contact their system administrator, network administrator, or department head for assistance. We committed to keep our constituency informed of potential vulnerabilities, and where possible, will inform this community of such vulnerabilities

before they are actively exploited.

2.2 Incident Handling

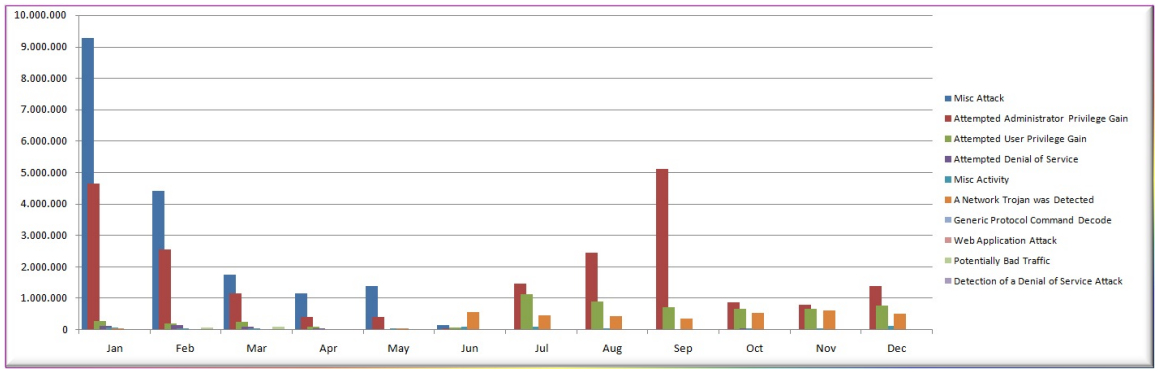
Assisting +20 Cyber Crime case with INP as an expert witness and +50 technical support and incident analysis/handling.

2.3 Incident Statistic

Based on our Monitoring Systems below is 10 Most Active events:

Classification	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Misc Attack	9.265.759	4.412.183	1.751.258	1.161.333	1.407.615	154.060	406	2.081	1.539	6.984	10.808	4.770
Attempted Administrator Privilege Gain	4.653.292	2.549.203	1.161.362	416.932	402.630	40.867	1.463.948	2.461.394	5.127.160	884.703	800.065	1.402.242
Attempted User Privilege Gain	287.568	215.619	257.479	96.806	31.501	68.107	1.135.140	892.301	732.629	683.432	667.075	769.397
Attempted Denial of Service	118.416	154.191	106.304	42.294	140	29.588	19.351	24.342	26.192	38.960	16.079	20.893
Misc Activity	68.331	50.031	62.414	32.951	39.218	105.934	91.734	56.537	37.710	40.912	44.256	120.638
A Network Trojan was Detected	47.333	32.968	35.562	24.906	40.089	559.356	464.261	434.749	352.842	540.480	624.202	507.928
Generic Protocol Command Decode	11.631	8.263	5.625	716	557	281	0	58	11	1.480	1.673	305
Web Application Attack	3.839	64	409	397	814	258	3.633	2.774	1.845	2.449	1.911	6.633
Potentially Bad Traffic	3.530	73.150	97.307	9.285	6.896	37	2.289	1.380	1.514	1.314	131	1.004
Detection of a Denial of Service Attack	642	546	303	0	0	0	0	0	1	0	81	0
TOTAL	14.460.341	7.496.218	3.478.023	1.785.620	1.929.460	958.488	3.180.762	3.875.616	6.281.443	2.200.714	2.166.281	2.833.810

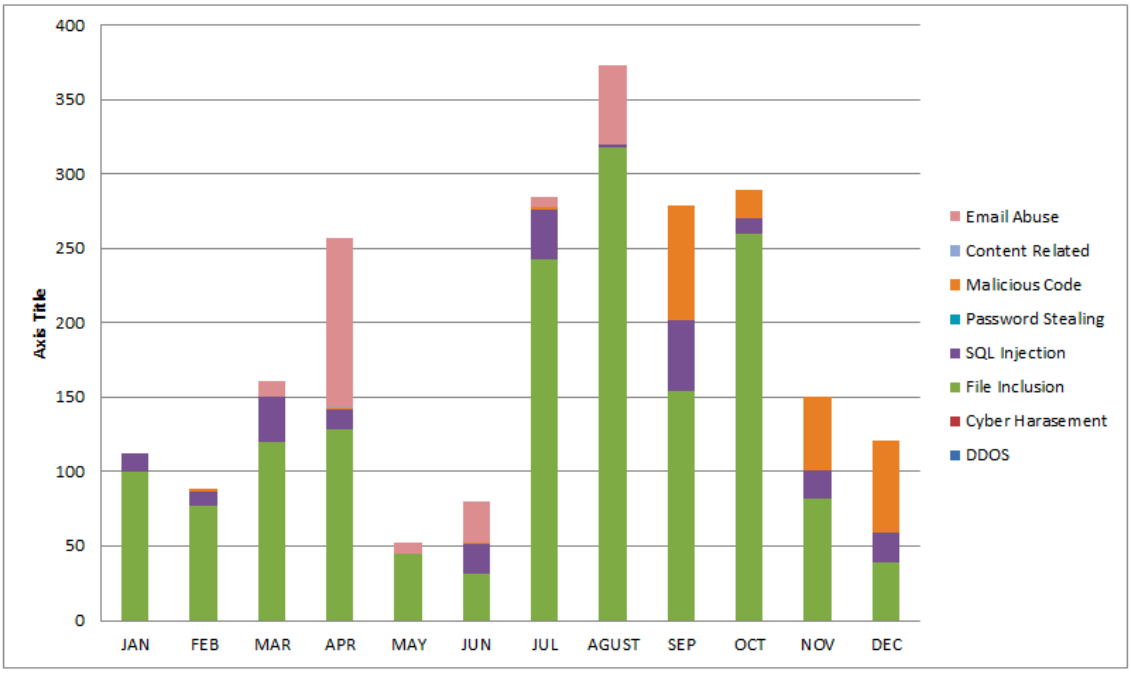
* 10 Active Events Classification



Based on indirect public reporting below is the type of incidents:

	BULAN											
TYPE OF INCIDENTS	JAN	FEB	MAR	APR	MAY	JUN	JUL	AGUST	SEP	OCT	NOV	DEC
DDOS												
Cyber Harasement												
File Inclusion	100	77	120	129	45	31	243	318	154	260	82	39
SQL Injection	12	10	30	13		20	33	2	48	10	19	20
Password Stealing												
Malicious Code		2		1		1	2		77	19	49	62
Content Related				1								
Email Abuse			11	113	7	28	7	53				

Description :	
Incident	
Normal	
In Progress	



2.4 Other Services

We conduct +50 various security training in 2011 i.e. Secure Coding and Secure Programming, Cyber Crime and Digital Forensic for LEA.

3. Event Organized/Co-Organized Achievement

3.1 International Membership

- FIRST, Full Member (2011)
- National CSIRT Forum (2010)
- APCERT, Full Member (2010)
- OIC-CERT, Full Member (2009)

3.2 Presentation and Publication

Security Awareness and Workshop Road Show in 5 major cities within the country and +20 seminars invitation.

3.3 Community Cooperation

Research and Development Project with APTIKOM – Academic CERT, National Honey Net, ID-X. Special Program with SANS, EC-COUNCIL, KKI and SGU.

4. International Cooperation

4.1 Memorandum of Understanding

- MYCERT/CC (renew)
- JPCERT/CC (renew)
- KRCERT/CC (on progress)
- CNCERT/CC (on progress).

4.2 Conference and Events

- AOTS Training 2011, Tokyo – Japan
- APCERT AGM 2011, Jeju – Korea
- FIRST AGM 2011, Vienna – Austria
- OIC-CERT AGM 2011, Dubai – UEA
- OIC-CERT Workshop 2011, Brunei
- Secure Programming, Tokyo – Japan.

5. Future Plans

- Put more monitoring sensors within 39 NAP
- Established Public Incident Reporting Service
- More Research and Development Cooperation
- More technical trainings and awareness program
- Supporting the establishment of sectors CSIRT
- Assisting LEA to overcome the growth of cyber crimes
- Suggestions for improvement of regulations and future cyber legislation
- Providing technical support and assistance for security implementation in the critical infrastructure sectors.

6. Conclusion

In 2011, there was no large-scale network security incident happened with mass damage, but it is very important to increase attention level to issues affecting critical infrastructure. Thus, it is necessary for government, ISPs, Sociaties, Internet users, to pay much more attention and cooperate with one another more effectively. Id-SIRTII/CC is also in need of increasing the number of collaboration with CERTs community from all over the world to prevent and mitigate the impact of any cyber

threat.

9. JPCERT/CC Activity Report

Japan Computer Emergency Response Team / Coordination Center - Japan

1. About JPCERT/CC

1.1 Establishment

JPCERT/CC is the first CSIRT (Computer Security Incident Response Team) established in Japan. It is an independent non-profit organization, serving as a national point of contact for the CSIRTs in Japan and worldwide. After its inception in 1992, JPCERT/CC was officially established in 1996, and has been conducting incident handling operations, vulnerability handling operations, engaging in malware and threat analysis, publishing security alerts and advisories to the wide public, organizing forums and seminars to raise awareness of security issues, and supporting the establishment and operations of CSIRTs in Japan and overseas.

1.2 Constituency

JPCERT/CC coordinates with network service providers, security vendors, government agencies, as well as the industry associations in Japan.

2. Activities & Operations

2.1 Incident Handling Reports

In 2011, JPCERT/CC received 7,722 computer security incident reports from Japan and overseas. A ticket number is assigned to each incident report to keep track of the status.

	1st Qtr	2nd Qtr	3rd Qtr	4th Qtr	Total
Incident Reports	1,936	1,567	1,718	2,501	**7,722**

Figure 1. Incident reports to JPCERT/CC (2011)

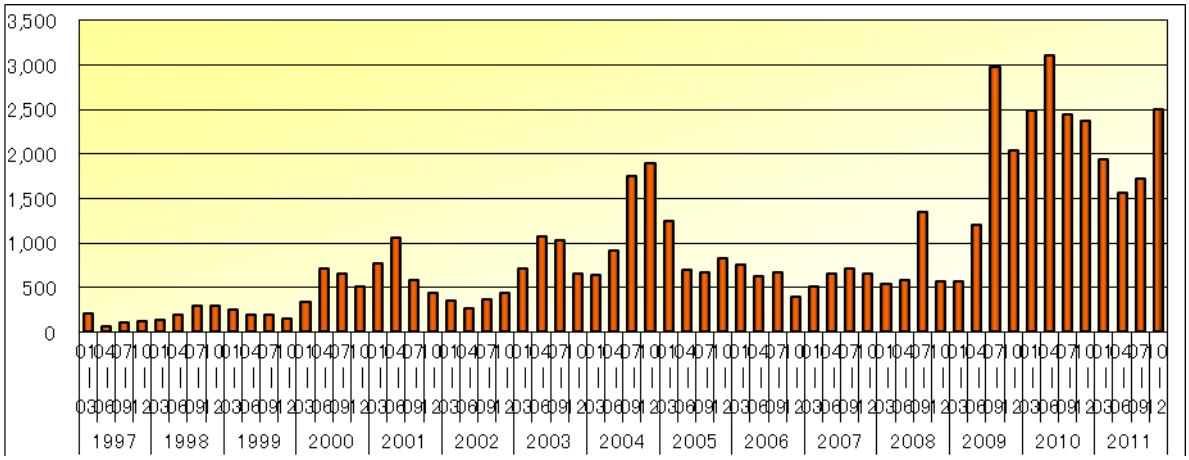


Figure 2. Incident reports to JPCERT/CC (1997-2011)

2.2 Abuse statistics

The incident reports to JPCERT/CC in 2011 were categorized as in Figure 3. More than half of the incident reports were on scan, followed by phishing and malware.

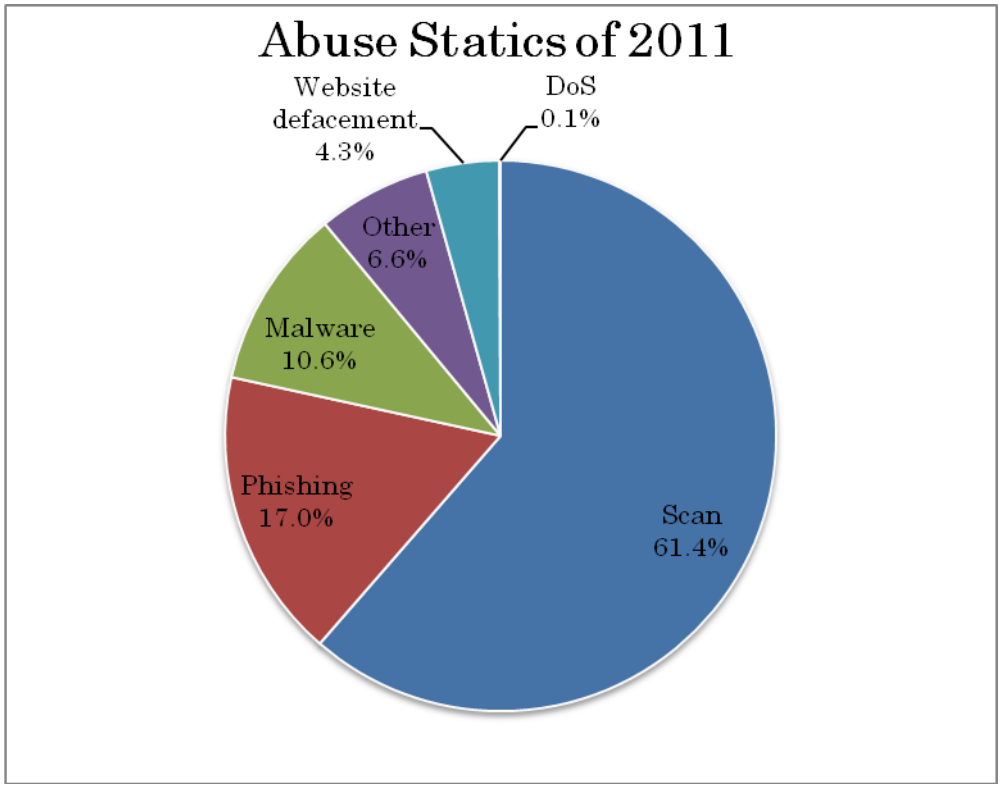


Figure 3. Abuse Statistics of 2011

2.3 Security Alerts and Advisories

- Security Alerts

https://www.jpcert.or.jp/at/ (Japanese)
https://www.jpcert.or.jp/english/at/ (English)
JPCERT/CC publishes security alerts on widespread, emerging information security threats and their solutions, on an as-needed basis. In 2011, 45 security alerts were published.

- **Early Warning Information**
  JPCERT/CC publishes early warning information to the Japanese government and to organizations providing national critical infrastructure services and products. Early warning information contains information on threats, threat analysis and their solutions.

- **Japan Vulnerability Notes (JVN)**
  https://jvn.jp/ (Japanese)
  https://jvn.jp/en/ (English)
  JVN is a vulnerability information portal site that provides vulnerability information and their countermeasures for software products used in Japan. JVN is operated jointly by JPCERT/CC and the Information-technology Promotion Agency (IPA) and provides the descriptions, solutions, and developers' statements (including information on affected products, workarounds and solutions, such as updates and patches) on each vulnerability.
  JPCERT/CC conducts vulnerability handling operations cooperatively with CERT/CC (http://www.cert.org/), CPNI (http://www.cpni.gov.uk/) and CERT-FI (http://www.cert.fi/en/).
  In 2011, 267 vulnerabilities coordinated by JPCERT/CC were published on JVN. Among them, 114 cases were reported through IPA in Japan, and 153 cases were published in cooperation with CERT/CC.
  In June 2010, JPCERT/CC became a CVE Numbering Authority (CNA). Since then, JPCERT/CC is releasing Japan Vulnerability Notes (JVN) and JVN iPedia entries that contain reserved CVE Identifier numbers.

  - JPCERT/CC Becomes CVE Numbering Authority (Japanese)
  https://www.jpcert.or.jp/press/2010/PR20100624_cna.pdf
  - JPCERT/CC Becomes CVE Numbering Authority (English)
  http://cve.mitre.org/news/archives/2010_news.html#jun232010a

- **JPCERT/CC Weekly Report**

  JPCERT/CC publishes weekly reports on selected security information of the preceding week that is regarded as high importance by JPCERT/CC. Weekly reports also contain a relevant security tip every week.

- **JPCERT/CC on Twitter**

  http://twitter.com/jpcert (Japanese)

  http://twitter.com/jpcert_en (English)

  Since January 2009, JPCERT/CC is providing information security related alerts via Twitter.

- **JPCERT/CC Official Blog**

  http://blog.jpcert.or.jp/ (English)

  Since September 2010, JPCERT/CC is providing security news regarding Japan as well as activities happening at JPCERT/CC on an English language blog.

2.4 Control System Security

JPCERT/CC coordinates control system security with relevant organizations in Japan. It provides information on vulnerabilities and solutions regarding control systems, lists of recommended reading materials, as well as reports and documents.

2.5 Analysis Center

JPCERT/CC has a research center for conducting technical examination and analysis of artifacts. The artifacts include not only viruses and bots but also tools which can potentially be used with malicious intent. As the findings though the analysis are incorporated into the incident response and the information provision that forms the basis of JPCERT/CC, our research center is pursuing the sophistication of the analysis environment and its capability.

2.6 Education / Public Awareness

- **Secure Coding**

  JPCERT/CC provides C/C++ secure coding seminars, CERT C Secure Coding Standards, books and materials on secure software development and secure

coding rules. It is scheduled that from 2012, JPCERT/CC will provide Java/Android Secure Coding Seminar.

- **Technical Notes**
  JPCERT/CC publishes documents that provide general technical information and/or instructions for incident handling.

- **Library**
  The library provides security materials targeting both security professionals and beginners, such as information security materials for new employees, security setup of e-mail software, professional security review, etc.

2.7 Internet Scan Acquisition System (ISDAS)

https://www.jpcert.or.jp/english/isdas/

ISDAS monitors the Internet traffic in Japan in order to detect threat activities such as worm and scan. The project was initiated in November 2003 with the objective of improving Internet security by providing up-to-date graphs and reports.

2.8 TSUBAME (Internet Threat Monitoring Data Sharing Project)

The TSUBAME project is designed to collect, share and analyze Internet traffic data, in order to understand the Internet threat situation in the Asia Pacific region. It deploys sensors widely in the region, collecting and sharing the data with all participating teams. The TSUBAME project aims to establish a common platform to promote collaboration among CSIRTs in the Asia Pacific region. TSUBAME Working Group is active in APCERT and observation results are frequently exchanged among the teams.

2.9 Associations, Projects and Communities

- **Nippon CSIRT Association**
  http://www.nca.gr.jp/index.html (Japanese)
  This association is a community for CSIRTs in Japan. JPCERT/CC serves as the secretariat for the association.

- **Council of Anti-Phishing Japan**
  https://www.antiphishing.jp/ (Japanese)

JPCERT/CC serves as the secretariat for the Council of Anti-Phishing Japan.

- **Cyber Clean Center (CCC)**
  https://www.ccc.go.jp/en_index.html
  From December 2006 to March 2011, Cyber Clean Center (CCC) acted as a core organization taking a role to promote BOT cleaning and prevention of re-infection of users' computers in Japan which are once infected by BOTs, based on cooperation with local ISPs (Internet Service Providers).
  The project was coordinated by the Ministry of Internal Affairs and Communications (MIC) and Ministry of Economy, Trade and Industry (METI). JPCERT/CC contributed to the project by analyzing malware and developing disinfection tools for infected users.

3. Events

3.1 Trainings, Seminars and Workshops

JPCERT/CC offers trainings, seminars and workshops, for technical staffs, system administrators, network managers, etc. Some of the events organized by JPCERT/CC in 2011 are as follows:

Invitational Training	-CSIRT Training Course for Asia Pacific (January)
On-site Training/Seminar	-TSUBAME Workshop (March) -C/C++ Secure Coding Seminars (May) -CSIRT Training Course for Africa (May and November) -Network Forensics Training for Myanmar (September) -Malware Analysis Training for Myanmar (December)
Domestic Seminars/Conference	-Control System Security Conference (February) -C/C++ Secure Coding Seminars (January, February, March) …and many more

3.2 Dispatch of Experts and Speakers

JPCERT/CC dispatches experts and speakers abroad. Below are the events where our experts were dispatched.

Dispatch of Experts	-Support of PacCERT establishment (July-)
Dispatch of Speakers	Taiwan Internet Trend Seminar 2011 (March) APSTAR Retreat (September) The 2nd APT Cybersecurity Forum (December) …and many more

3.3 Participation to International Events

JPCERT/CC participates in the many international events. Below are the events we joined in 2011:

BlackHat DC 2011 (January)

RSA Conference 2011 (February)

APSTAR Retreat (February)

CansecWest (March)

APWG Conference (April, November)

INT'L SOFT CHINA 2011(May)

Industrial Control Systems Joint Working Group (ICSJWG) Conference (May, October)

23rd Annual FIRST Conference Vienna (June)

National CSIRT Meeting (June)

Workshop on the Economics of Information Security (WEIS) (June)

The 3rd ASEAN-Japan Government Network Security Workshop (September)

Control Systems Cyber Security Advance Training and Workshop (September)

Society of Instrument and Control Engineers (SICE) Annual Conference (September)

GOVCERT.NL Symposium2011 (November)

CIP-Forum (November)

…and many more

3.4 Drills

JPCERT/CC participated in the following drills in 2011 to test our incident response capability:

- APCERT Drill 2011 (22 February)
- ASEAN CERT Incident Drill (ACID) 2011 (27 September)

4. MoU

To further strengthen cooperation, JPCERT/CC has been signing a Memorandum of

Understanding (MoU) with various security organizations. For 2011, MoU between CNCERT/CC, JPCERT/CC and KrCERT/CC was signed on 20 December.

5. Other Publications

JPCERT/CC also publishes quarterly activity reports, study/research reports, and CSIRT related materials.

6. International Contribution

- **FIRST (Forum of Incident Response and Security Teams)**
  http://www.first.org
  JPCERT/CC contributes to the international CSIRT community by serving as a Steering Committee member of the FIRST organization, since 2005. JPCERT/CC is offering sponsorship support for CSIRTs who wish to be the member of FIRST.

- **ISO International Standard**
  (ISO/IEC JTC 1/SC 27 Information technology – Security techniques)
  JPCERT/CC contributes to the following ISO International Standards being developed under ISO/IEC JTC 1/SC 27:
  ISO/IEC 29147: "Vulnerability Disclosure"
  ISO/IEC 27035: "Information Security Incident Management"
  ISO/IEC 30111: "Vulnerability Handling Processes"

- **APCERT (Asia Pacific Computer Response Team)**
  http://www.apcert.org/
  Since its establishment, JPCERT/CC has been acting as the secretariat for the organization. Beginning in March 2011, JPCERT/CC has been serving as the Chair team. JPCERT/CC is also the convener of the TSUBAME Working Group, which is aimed to establish a common platform for Internet threat monitoring, information sharing & analyses within the region.

7. JPCERT/CC Contact Information

URL: https://www.jpcert.or.jp/
E-mail: global-cc@jpcert.or.jp

Phone: +81-3-3518-4600

Fax: +81-3-3518-4602

10. KrCERT/CC Activity Report

Korea Internet Security Center - Korea

1. About KrCERT/CC

1.1 Introduction

Korea Computer Emergency Response Team/Coordination Center(KrCERT/CC) serves as the focal point to coordinate security incidents on all Korean constituency. In the national cybersecurity framework, KrCERT/CC, under Korea Communications Commission(KCC), covers the incident handling and security of information systems and networks in private sector such as telecommunication sector and home users. Internationally, KrCERT/CC cooperates with many leading national CSIRTs, international organizations, security vendors and so on.

1.2 History

KrCERT/CC established in 1996 and joined in FIRST(Forum of Incident Response and Security Teams), the only global CSIRT forum, in 2008 as the first Korean member.

KrCERT/CC has responded to many security challenges and evolved itself to meet those challenges. The first major challenge is the breakdown of Internet infrastructure over several hours caused by slammer worm outbreak on 25th January 2003. At that time, KrCERT/CC didn't have the effective communication and coordination system in place yet. Korean government recognized that the close collaboration between CERT and ISP is a key success factor for major incidents. Korea Internet Security Center(KISC), 24/7 security operation center, started the operation in December 2003.

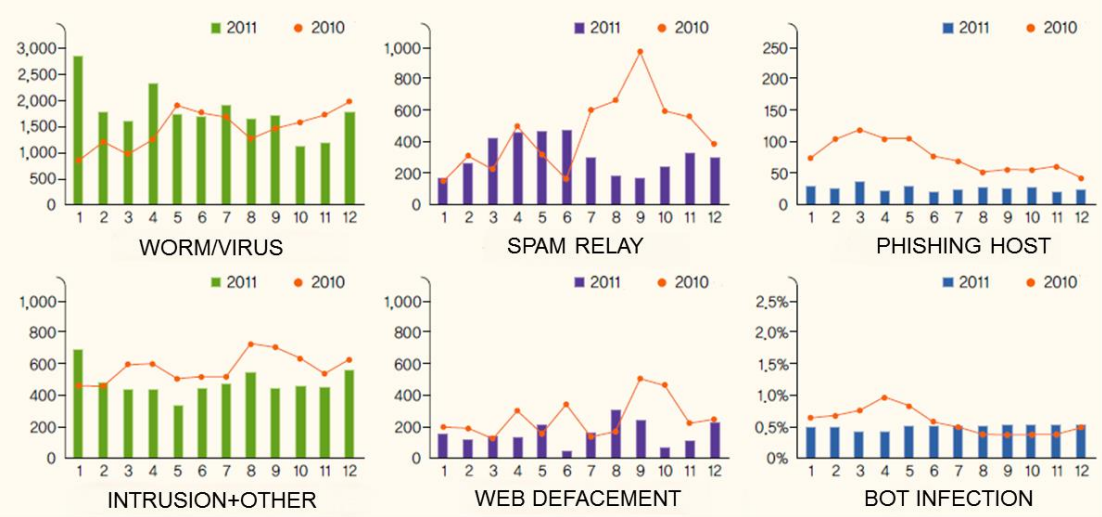
Distributed Denial of Service(DDoS) attack targeting Korea and US government in July 2009 was another big challenge from KrCERT/CC. Response experience with this DDoS attack enabled KrCERT/CC to improve its capability and operation. To do so, much budget was approved for CSIRT operation improvement and new staffs were hired. As a result, new services, such as DDoS shelter, cyber remediation service and so on, were introduced.

In 2011, KrCERT/CC enlarged the incident prevention functions to balance response and prevention activities. The prevention division consisted of 4 teams: incident prevention planning, IT service infrastructure protection, Advanced Technology development and Security R&D.

2. ACTIVITIES IN YEAR 2011

2.1 Incident handling reports

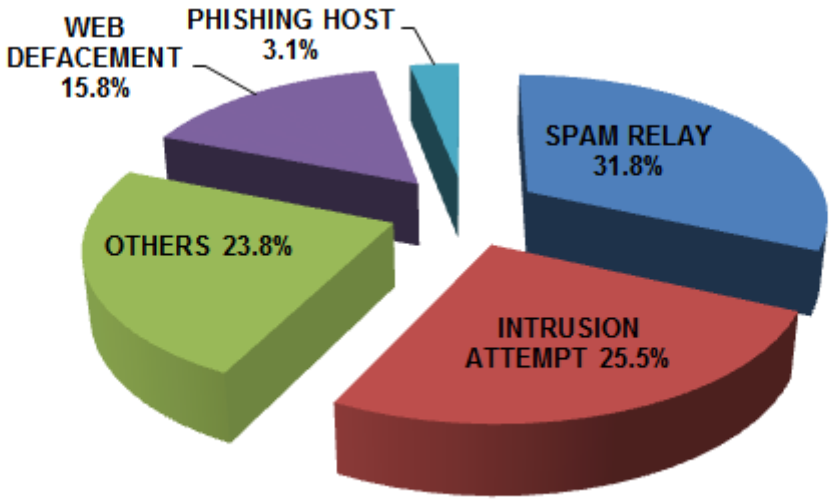
Internet incidents reported to KrCERT/CC are classified into the following 3 categories: worm/virus, hacking incident and bot infection. Hacking incident is classified into 4 sub-categories: spam relay, phishing host, intrusion attempt and web defacement.



2011 KrCERT/CC incident report statistics

The number of incident reports on worm/virus to KrCERT/CC in 2011 is 21,751. It is around 21 percent increase, compared to that of 2010(17,930). The monthly average number of incident reporting increased from 1494 in 2010 to 1,812 in 2011.

The number of hacking incident reported to KrCERT/CC decreased from 16,295 in 2010 to 11,690 in 2011. The number of spam relay subcategory decreased from 5216 in 2010 to 3,727 in 2011. The number of phishing host subcategory also decreased from 891 in 2010 to 365 in 2011.



2011 KrCERT/CC hacking incident report ratio

2.1.1 Worm/Virus

The number of worm/virus incidents reported to KrCERT/CC in 2011 is 21,751. The number of this worm/virus incident reports increases over years. The most reported malware in 2011 is ONLINE GAMEHACK, which steals the online game credential, such as ID and Password. The malware was also ranked no 1 in 2010. Bad guys or hackers try to gain the financial benefit by selling expensive online game items collected from stolen game accounts. The information can be traded in online black market. End users need to make efforts to prevent the damage from malware by installing up-to-date windows patches and scanning computers with the anti-virus vaccines.

2.1.2 Hacking Incident

The number of hacking incident reported to KrCERT/CC in 2011 is 11,690. All subcategories of the hacking incident decreased compared to 2010. Spam relay still takes the largest portion with 31.8%. Particularly, the number of phishing host reports drastically decreased from 891 in 2010 to 365 in 2011.

KrCERT/CC observes a new trend in phishing host. Phishing hosts targeting Korean organizations such as banks and so on located in foreign countries are reported frequently to KrCERT/CC. KrCERT/CC blocks the access to those foreign phishing hosts in cooperation with ISPs and send the request to take down phishing hosts to

the relevant CSIRTs or ISPs.

3. Events organized

3.1 2011 APCERT AGM & Annual Conference

KrCERT/CC successfully hosted 2011 APCERT AGM & Annual Conference in Jeju island from 22 to 25 March 2011. 115 Attendees from 17 economies joined in the events. The achievement can be summarized into endorsing the new vision, establishing 4WG(information classification, information sharing, membership and operational framework). KrCERT/CC took the role of membership WG convener.

Strategic planning meeting was organized to discuss APCERT future direction, including vision. New APCERT vision was approved during the AGM. This is one of big changes after APCERT was established.
KrCERT/CC was elected as the deputy chair to serve one year term 2011.

4. International Collaboration

KrCERT/CC signed memorandum of understanding(MoU) with foreign national CSIRTs and leading security company. Joint multilateral MoU among CJK(China-Japan-Korea) national CSIRTs was signed to broaden the cooperation boundary from bilateral one. The MoU with McAfee would enable KrCERT/CC to share cyber threat information with leading security companies.

5. Future Plans

KrCERT/CC will resume the hosting of APISC training course to support capacity building for CERT/CSIRTs from developing economies. KrCERT/CC continue working with foreign partners actively on diverse issue on cyber security.

KrCERT/CC Contact Information

Website : http://www.krcert.or.kr/english_www

E-mail : first-team@krcert.or.kr

Phone : +82-2-118

1.0 MALAYSIA COMPUTER EMERGENCY RESPONSE TEAM (MyCERT)

1.1 Introduction

MyCERT, which stands for **Malaysia Computer Emergency Response Team**, was established nearly 15 years ago with the aim of mitigating computer security concern of the Malaysian Internet users. It acts as a point of reference in handling computer security incidents in its constituency that is overwhelm in utilizing the Internet for acquiring information, socializing and performing commerce.

In 2011, MyCERT observed an increase of 88 percent compared to the previous year in computer related incidents reported through its Cyber999 help centre. Base on this increment, it can be concluded that the computer incidents are increasing and/or more the computer users are aware of the existence MyCERT for computer incident reporting.

Apart from providing the Cyber999 services, MyCERT also operates a Malware Research Centre that perform researches on malware as well as issue alerts and advisories to its constituency.

In dealing with computer security, it is essential to have strong collaboration with the international computer security incident response teams (CSIRTs) and as such, MyCERT affiliates itself with the Asia Pacific Computer Emergency Response Team (APCERT) and the Organization of Islamic Cooperation - Computer Emergency Response Team (OIC-CERT). Since APCERT's establishment in 2003, MyCERT as a founding member, has actively cooperated in events that allows for enhanced cooperation, knowledge sharing and development of teams operational capability.

1.2 Establishment

MyCERT, established in 13th January 1997, is a department of CyberSecurity Malaysia, the national cyber security specialist centre under the purview of the Ministry of Science, Technology and Innovation (MOSTI), Malaysia. CyberSecurity Malaysia main roles can be summarized as follows:

- To assist MOSTI in the implementation of the National Cyber Security Policy (NCSP)
- To provide Cyber Security Emergency Services and act as the national technical coordination centre
- To conduct Cyber Threat Research & Risk Assessment
- To provide Cyber Security Quality Management Services
- To build capability in the field of cyber security (Training) and to create awareness and a culture of cyber security (Outreach)

Further information about CyberSecurity Malaysia can be viewed at:
http://www.cybersecurity.my/en/

1.3 Workforce

MyCERT currently has 22 dedicated staff operating its two main services, the Cyber999 Security Incident Help Centre and the Malware Research Centre. However, as CyberSecurity Malaysia, there are about 200 staffs that provide MyCERT support in various cyber security initiatives.

1.4 Constituency

MyCERT's constituency is the Malaysian Internet Users. Incidents within Malaysia that are reported either by the Malaysian public or international organizations will be resolved by assisting the complainants on technical matters. If a case involves international connection, then MyCERT will request trusted parties in that particular country or constituency to assist in resolving the security issues.

2.0 ACTIVITIES IN YEAR 2011

As in previous years, MyCERT involvements in cyber security activities were lively due to participation in various national and international security events and especially in handling security incidents that had increased twofold from 2010.

2.1 Incident Handling

Computer security incidents taken up by MyCERT were made through proactive monitoring on specific incidents, as well as through incidents reported by various parties within its constituency which include home users, private sectors as well as

government sectors and external parties outside the constituency involving users, security teams from abroad, foreign CERTs as well as Special Interest Groups (SIG).

For 2011, MyCERT had handled a total of 15,218 security incidents reported via the Cyber999© Help Centre, almost double from the previous year. Approximately 97% of these incidents were resolved according to the centre's service level agreements (SLAs). At the same time, about 4,877 of incidents related to malware, intrusion attempts, infection attempts and remote file inclusion (RFI) attacks were processed by the Malware Research Centre. More information on the incidents can be viewed at:

http://www.mycert.org.my/en/services/statistic/mycert/2011/main/detail/795/index.html

MyCERT had issued 28 security alerts related to various vulnerabilities in applications and and four MyCERT Quarterly Summaries in 2011. The list of alerts and summaries can be viewed at:

http://www.mycert.org.my/en/services/advisories/mycert/2011/main/index.html

2.2 Abuse Statistics

MyCERT's monthly abuse statistics is based on security incidents generally categorized as below:

- Malicious code (Botnet C&C, Bots, Malware, Malware hosting)
- DOS (DOS)
- Fraud (Phishing, Fraud site, Fraud purchase, Counterfeit item, Online scam, Unauthorized transaction, Lottery scam, Nigerian scam, Job scam)
- Intrusion Attempt (Port scanning, Login brute force, Vulnerabilities probes)
- Cyber Harassment (Cyber bullying, Cyber stalking, Sexual, Religious, Racial)
- Content Related (Pornography, Intellectual property, National threat)
- Intrusion (Account compromise, Defacement)
- Spam (Spam, Spam relay)
- Vulnerabilities Report (Misconfiguration, Web, System)

In 2011, MyCERT had seen a significant increase in reports concerning fraud,

intrusion and spam. The figures below shows reported cases that were handled by MyCERT for the year under review:

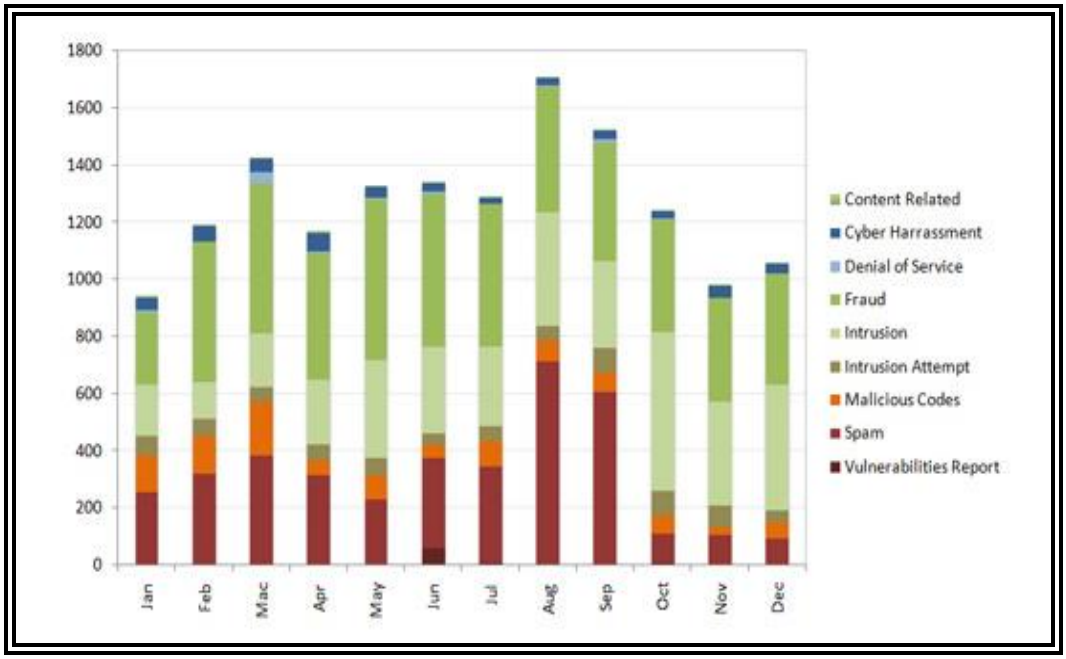


Figure #1: Reported Incidents Handled by MyCERT in 2011

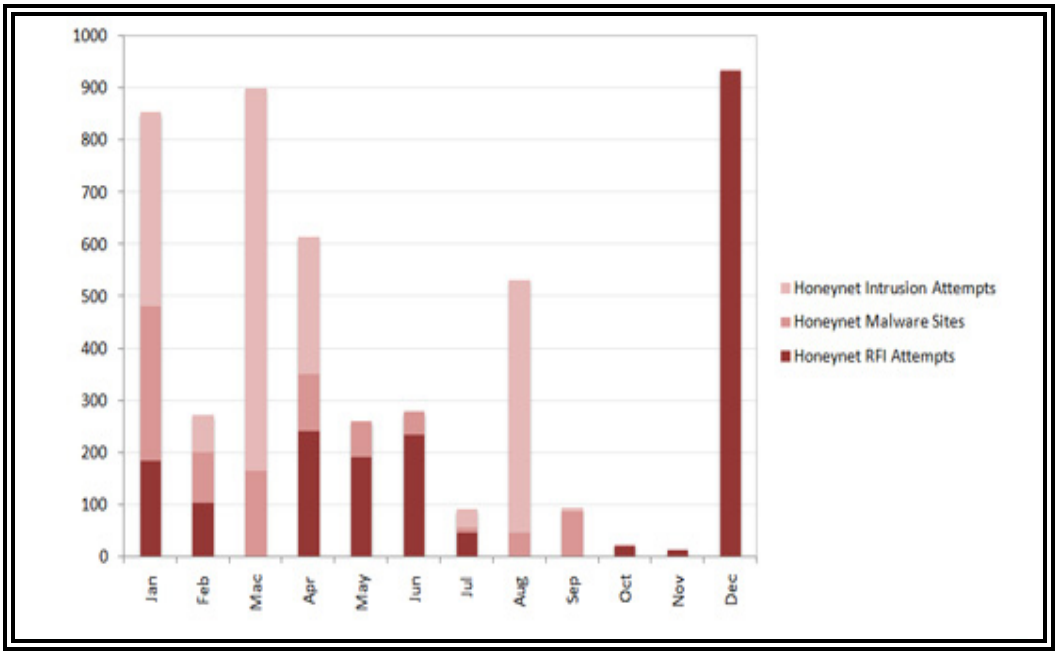


Figure #2: Honeynet Project Related Incident Statistics in 2011

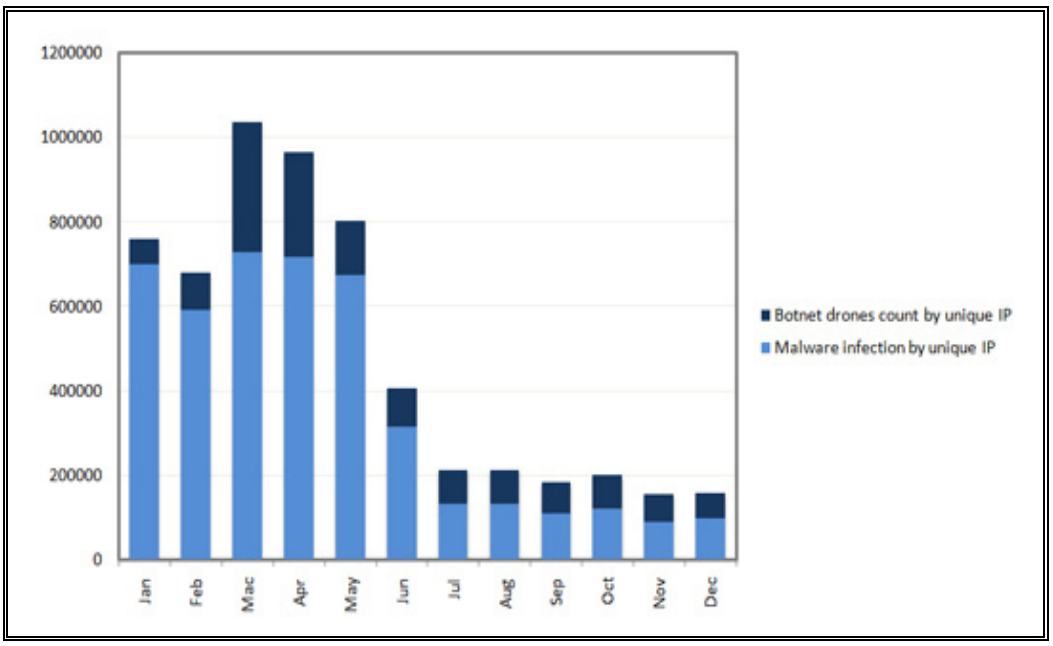


Figure #3: Botnet Drones and Malware Infection in 2011

2.3 Trainings

Several workshops or hands-on training were conducted by MyCERT 2011 which include:

- Analyzing Malicious PDF, HonetNet project, Paris, France
- Reversing Engineering Android Malware, HonetNet project, Paris, France
- Web Security, SAHNET Honeynet, Damman, Saudi Arabia
- Analyzing Malicious PDF, SAHNET Honeynet, Damman, Saudi Arabia
- Reversing Engineering Android Malware, ISSUMMIT, Hong Kong
- Incident Handling and Security, OIC-CERT, Brunei

MyCERT had also conducted several local training related to web security, and incident handling for local security organizations.

2.4 Cyber Security Exercises

In maintaining and assessing MyCERT's incident handling SOP and best practices, MyCERT had participated in cyber exercises as organizer and/or player. The significant of having the exercise was to further strengthen the cooperation and capabilities among participating agencies. Three cyber-drills of national and

international significant in 2011 involving MyCERT are;

- The Asia Pacific CERT (APCERT) Drill
  MyCERT participated as a player as well as taking the role of the exercise advisor in this drill organized on 22 Feb 2011.

- ASEAN CERT Incident Drill (ACID)
  MyCERT participated as a player in the drill organized on 27 Sept 2011.

- National Cyber Drill (X-Maya 4)
  CyberSecurity Malaysia through MyCERT had cooperated with the National Security Council (NSC) in planning, coordinating and developing the drill scenarios and artifacts for X-Maya 4, the 4th annual national cyber security exercises. 52 agencies from 10 Critical National Information Infrastructure (CNII) sectors participated in the cyber drill on 15th Nov 2011.

2.5 Seminars & Conferences

CyberSecurity Malaysia, through MyCERT, had co-operated with the Anti Phishing Working Group (APWG) in organizing the fifth annual Counter-eCrime Operations Summit (CeCOS V) on 27-to-29 April 2011 in Kuala Lumpur Convention Centre. The focus of the event was on the development of response paradigms and respires for the counter-ecrime managers and forensic professionals.

3.0 ACHIEVEMENTS

3.1 Presentation

MyCERT representatives had been invited to various talks at international conferences or seminars as speaker. Among the distinguished events were:

- APWG – The fifth annual Counter-eCrime Operations Summit (CeCOS V), Malaysia
- 3rd APEC Seminar on Protection of Cyberspace, Seoul, South Korea

- SAHNET Honeynet, Damman, Saudi Arabia
- SWISS CyberStorm, Zurich, Switzerland
- HITCON 2011, Taipei, Taiwan
- DEFCON, Nevada, USA
- HITBSec2011KUL, Kuala Lumpur, Malaysia
- APEC TEL 44, Kuala Lumpur, Malaysia

In addition to the above, MyCERT had spoken at not less than 10 other different international and local events throughout the year.

3.2 Publications

In order to enhance the capability in expressing knowledge in the form of literature, MyCERT members had produced some publication to share their knowledge.

- Academic Journal
  - Metaware - An extensible malware detection and removal toolkit (http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=5745976)
  - Automated blocking of malicious code with NDIS Intermediate Driver (http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=5745908)
- Articles
  - Reversing Android Malware: Geinimi Analysis
  - TipsFromTheLab e-zine

3.3 Certification

2011 saw 10 of MyCERT members being certified the prestigious SysAdmin, Audit, Network, Security (SANS) Institute with three for SANS GREM (Reverse Engineering) and six for SANS GCIH (Incident Handling) and one for SANS GWAPT (Web Penetration).

3.4 Security Tools Development

MyCERT under the Malware Research Centre (MRC) had made a breakthrough in the development of security tools to be used by the public and its internal team.

There were seven tools that were developed in 2011:

- DNSWatch
  http://www.mycert.org.my/en/resources/security_tools/main/main/detail/827/index.html
- MyPHPIPS
  http://www.mycert.org.my/en/resources/security_tools/main/main/detail/828/index.html
- Shellcode Analyzer (For MyCERT only)
- DNSMon v2 (For MyCERT only)
- Dashboard (For MyCERT only)
- Bot tracker (IRC, HTTP)
- WPScan's module

The MRC unit had also updated the existing tools it had developed last year such as the:

- Gallus
- DontPhishme
- Pkaji
- RFIPot (host bypass, host blacklist)

4.0 INTERNATIONAL COLLABORATION

To maintain sound cooperation among security organization, MyCERT had collaborated with several new agencies. This is expected to further strengthen its capability in order to mitigate security threats in the cyber security arena.

4.1 Membership Support

As was in previous years, MyCERT had the opportunity to support other teams that would like to be recognized within the Computer Incident Response network especially in FIRST and APCERT. The teams sponsored were:

- Teams supported to become APCERT member

- Myanmar Computer Emergency Response Team (mmCERT)

- Teams supported to become FIRST member
  - Maybank Computer Emergency Response Team (MBBCERT)
  - Egypt Computer Emergency Response Team (EG-CERT)

4.2 New Partnership and Existing Cooperation

2011 saw new partnerships made with international and national security organizations. The cooperation were mostly made with closed security groups, governmental agencies, CSIRTs, and academic institution.

In being accepted as an established security agency in APCERT, MyCERT was reappointed as the Steering Committee (SC) member in APCERT.

Further to this, CyberSecurity Malaysia was also reappointed as the Chair and SC member of the Organization of the Islamic Conference – Computer Emergency Response Teams (OIC-CERT).

It also maintained its Full Member status in the Forum of Incident Response Security Team (FIRST).

5.0 FUTURE PLANS

5.1 Future projects

To assist the nation and the Internet users from being a victim to cyber attacks, MyCERT is looking at new development and innovation of security tools especially in mobile malware research, ROP shellcode and web protection applications.

6.0 CONCLUSION

As per past operation, the year 2011 had provided considerable experience required for the team to further strengthen its reactive and proactive services to its

constituency. MyCERT had actively assisted computer users in handling security incidents in addition to securing the nation from excessive cyber attacks from within and outside Malaysia.

With new emerging technology especially in the mobile field, the challenge for MyCERT as well as the international security field would certainly be securing IT hardware users from being attack. With an expected increase of Internet users, improvement of the security tools are required to be developed.

MyCERT with the support from other services in CyberSecurity Malaysia is looking forward to be at the forefront in safeguarding the nation from cyber threats. Cooperation from APCERT members and international security community is also expected to provide an interesting challenge for 2012.

12. SingCERT Activity Report

Singapore Computer Emergency Response Team - Singapore

1. About SingCERT

1.1 Introduction

The Singapore Computer Emergency Response Team (SingCERT) is a one-stop centre for security incident response in Singapore. Besides providing assistance to its constituency in incident resolution and co-ordination, SingCERT also broadcasts security alerts, advisories and security patches. To promote security awareness and to educate the general public, SingCERT organises regular seminars, workshops and sharing sessions covering a wide range of security topics.

1.1.1 Establishment

SingCERT was set up in 1997 to facilitate the detection, resolution and prevention of security related incidents on the Internet. SingCERT is a government funded national initiative, and is managed and driven by the Infocomm Development Authority of Singapore.

1.1.2 Constituency

SingCERT provides services primarily to the Singapore local constituency comprising of companies and end users.

2. Activities & Operations

2.1 Incident Trend

There is a decrease in the total number of incidents reported to SingCERT in the year 2011 as compared to the year 2010. In the previous year 2010, phishing websites especially of local banks were the major concerns. While phishing websites remained a major concern, in the year 2011, SingCERT was seeing a significant increase in the number of “Spear Phishing” incidents. These attacks were target specific and attackers customised the attacks accordingly with information that

will interest the victims, greatly increasing the chances of victims falling for the traps. SingCERT continues to work with other CERTs and our Internet Service Providers (ISPs) to track down affected users and keep them informed on how to secure their systems. On the regional and international fronts, collaboration and cooperation among CERTs have proved effective in the resolution of our cross-border incidents.

3. Events organised / co-organised

3.1 Seminars and Workshops

In our continued efforts to keep our constituency updated on security trends and developments, SingCERT organised 4 seminars and workshops for the year 2011. These events were co-organised with industry partners to bring the latest technology and knowledge to our security practitioners.

3.2 ASEAN CERTs Incident Drill 2011

The ASEAN CERTs Incident Drill (ACID) 2011 was conducted successfully on 27 September 2011. In order to develop scenarios which reflected prevailing cyber threats that were confronting the CERTs, the theme selected for the drill was focused on threats from Banking Windows Malware. 13 CERTs from 11 countries from ASEAN and Asia took part in the drill, and good feedbacks were received from all the participants.

4. International Collaboration

4.1 Incident Drill

SingCERT organised the ASEAN CERT Incident Drill in September 2011 and participated in the APCERT Annual incident drill in February 2011.

5. Future Plans and Projects

SingCERT will be organising the 7th ASEAN CERTs Incident Drill for the year 2012. Discussions are in progress to work out the scope and coverage.

Together with Australian Government AGD and CERT Australia, SingCERT will be co-hosting the ASEAN Regional Forum (ARF) Incident Response Workshop 2012. The event will be held in Singapore. The progress is still in the planning stage and information of the event will be finalised and released to the members shortly.

13. Sri Lanka CERT/CC Activity Report

Sri Lanka Computer Emergency Readiness Team / Coordination Center – Sri Lanka

1. ABOUT SRI LANKA CERT

1.1 Introduction

The Sri Lanka Computer Emergency Readiness Team | Coordination Centre (Sri Lanka CERT|CC) is the centre for cyber security in Sri Lanka, mandated to protect the nation's information infrastructure and to coordinate protective measures against, and responses to cyber security threats and vulnerabilities.

1.1.1 Establishment

As the national CERT of Sri Lanka, Sri Lanka CERT acts as the focal point for cyber security for the nation. It is the single trusted source of advice about the latest threats and vulnerabilities affecting computer systems and networks, and a source of expertise to assist the nation and member organizations, in responding to and recovering from Cyber attacks.

It was anticipated that cyber security incidents in Sri Lanka would increase dramatically due to IT infrastructure growth as a result of the National ICT Policy related activities, primarily, the e-Sri Lanka initiative and ICT revenue generation activities. Sri Lanka CERT therefore was established on 1st July 2006 as Sri Lanka's National CERT, by the ICT Agency of Sri Lanka (ICTA). ICTA is the Government Agency responsible for the development of IT Infrastructure and Policy in Sri Lanka. Sri Lanka CERT is registered as a Private Limited Liability Company, and is a fully owned subsidiary of the ICTA, which in turn is fully owned by the Government of Sri Lanka.

In early 2011, Sri Lanka CERT | CC, along with its parent body, the ICTA was brought under the purview of the newly formed Ministry of Telecommunications and ICT.

1.1.2 Workforce

Sri Lanka CERT currently has a total strength of ten team members consisting of the Chief Operating Officer, a Manager Operations, an Administrative Officer, a Senior Information Security Engineer and six Information Security Engineers. All the staff are highly skilled and experienced in different areas of information security and have achieved corresponding Information security certifications which are widely recognized in the industry, such as SANS GCIH, Microsoft MCSE, EC-Council Cerified Ethical Hacker (CEH) and Certified Hacking Forensics Investigator (CHFI), Cisco CCNA and CCSP and (ISC)² CISSP.

1.1.3 Constituency

Sri Lanka CERT's Constituency encompasses the whole of the cyber community of Sri Lanka (private & public sector organizations, and the general public). Sri Lanka CERT maintains a good rapport with government and private sector establishments, and extends assistance to the general public as permitted by available resources. In accordance with its mandate, Sri Lanka CERT | CC gives priority to requests for assistance from government. Based on availability of human resources and necessary skills, requests from private sector are handled free of charge or on a paid basis, depending on the type of service provided.

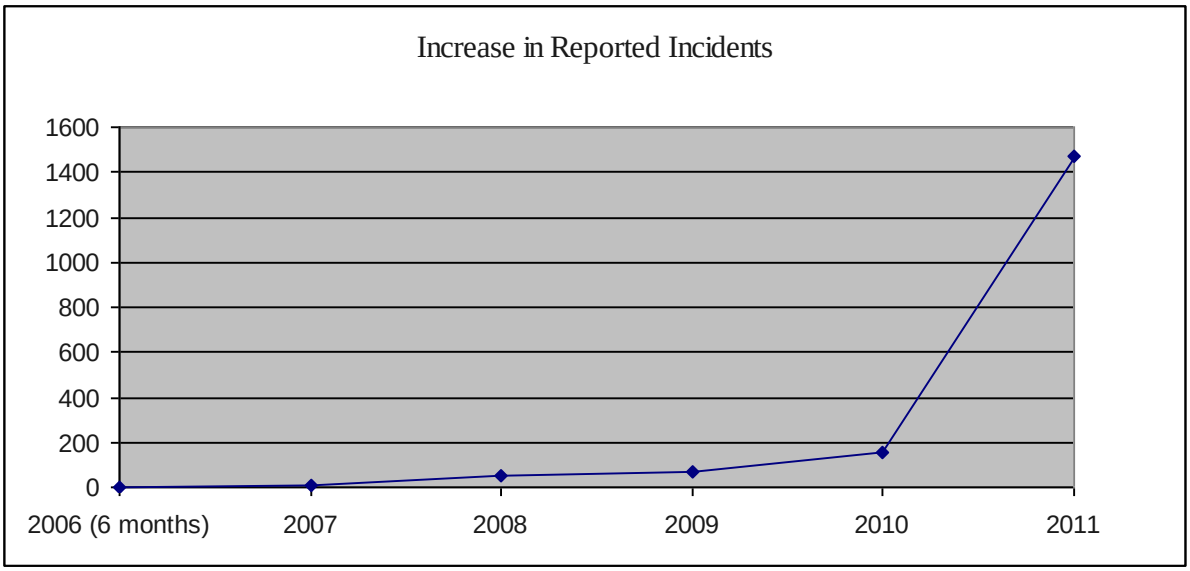
2. Activities & Operations

2.1 Incident Handling Statistics

Incidents reported to Sri Lanka CERT increased to 1469 in the year 2011. In the year 2010, only 151 incidents were reported. This can be seen as a major increase in the reported incidents compared to the year 2010. The following table depicts the distribution of various types of incidents reported to Sri Lanka CERT. All the incidents reported to Sri Lanka CERT have been resolved satisfactorily.

Type of Incident	No
Phishing	6
Abuse/Privacy	2
Scams	3
Malware	1
Defacements	20
Hate/Threat Mail	3
Unauthorized Access	3
Intellectual property violation	5
DoS/DDoS	1
Fake Accounts	1,425
Total	**1,469**

The following graph depicts the increase in the number of incidents since the inception of Sri Lanka CERT in mid-2006.



2.2 New services

2.3.1 Setting up sector based CSIRTs

Sri Lanka CERT has initiated the setting up of CSIRTs which are sector-based. Typical sectors are Banking, Telecom, Defence and Education. The Bank CSIRT is already operational while the Telco CSIRT concept paper is awaiting approval from the TRCSL Board, which is its intended host body. The other two CSIRTs are in the concept phase.

The rationale for sector based CSIRT's is to ensure that Sri Lanka CERT remains a small, focused national body that functions only as an incident escalation and coordination point and ensures national readiness to tackle large scale incidents effectively.

The net result of setting up sector based CSIRTs and certifying and coordinating the activities of these CSIRTs is that Sri Lanka CERT has now transformed itself to being a true coordinating body. The Board of Directors of Sri Lanka CERT has therefore recently approved the re-alignment of Sri Lanka CERT by re-naming itself as "Sri Lanka Computer Emergency Readiness Team" in addition to being the Coordinating Centre. This process is already underway and Sri Lanka CERT will soon be known as Sri Lanka CERT|CC.

Sector-based CSIRTs will provide industry specific services to their constituents. For example, The Telco CSIRT will provide content filtering services to ISPs while Bank CSIRT provides vulnerability alerts specific to banking software and implements security standards to ensure a minimum level of security compliance within the industry.

2.3.2 Incident handling - blocking Phishing sites

Since it takes considerable time to take down the phishing sites targeting local banks of Sri Lanka, a new process was established to block the sites locally with the

help of TRC (Telecommunication Regulatory Commission) Sri Lanka and the ISPs. This will minimize the damage that can be happen to local customers during the time of taking down those phishing sites with the help of international CERTs and ISPs.

2.3.3 National Certificate Authority

The Electronic Transactions Act no. 19 of 2006, creates a foundation for the existence of a national certificate authority. With the launch of the first e-citizen services and the increased use of online banking and other e-commerce facilities, the use of a digital ID is becoming more important. While LGN CA and Lanka Sign exist, the universal acceptance of their certificates is in question. To address this issue, Sri Lanka CERT, ICTA and various stakeholders have come together to form a task force to determine the policies, procedures, governance and service models of the national CA. The end objective is to have a national level body which will effectively regulate the issuing of a number digital certificate classes at affordable prices that are in accordance with the local legislation and international standards.

2.3.4 Vulnerability Assessments – Formal procedure for security testing government websites

Given several issues where timelines far exceeded acceptable levels when security testing government websites and applications, Sri Lanka CERT, ICTA, GIDC NOC conferred and established a formal procedure for strictly managing the process for security testing government web applications.

3. Events organized / co-organized

3.1 Training / Education

In order to fulfill its mandate to create awareness and build IS skills within the constituency; Sri Lanka CERT continues to organize training programs and education sessions targeting various audiences including CIOs, Engineers, System Administrators, Banking and Telecom Sector Staff, Students, and General Public.

During the year 2011 Sri Lanka CERT conducted the following training and education programs successfully:

a. Seminar series on "Internet safety for School Children" for School Children
b. Train the trainer program at National Colleges of Education on "Online Safety"
c. Presentation on "Penetration Testing"
d. Presentation on "Cyber security" for government CIOs
e. Presentations on "cooperation between incident response teams" and "Role of Incident response teams"
f. Presentation on "e-Government Information Security"

3.2 Consultancy

Sri Lanka CERT continues to provide consultancy services in response to requests made – particularly from government departments.

Typical consultancy services provided during the year 2011 included;

a. Security Policy development workshops for government organizations
b. Forensics investigation support for Law enforcement
c. Providing training for Digital Forensics Laboratory staff of the Police Department
d. Configuration reviews for critical government organization information systems
e. Virtualization security and migration consultancy to the Institute of Policy Studies (IPS)
f. Consultancy on security integration in to procurement processed for Sri Lanka Credit Insurance Corporation (SLECIC) and IPS
g. Formulation on organizational Information Security policy for SLECIC

3.3 Seminars & Workshops

a. End-user Security workshop for a government organization

b. Workshops on "Virtualization Cloud Computing and Next Gen Enterprise Architecture" and "Network traffic analysis"

This was conducted for the technical and information security staff of private and government sector organizations.

c. 4th Annual National Conference on Cyber Security 2011

This "Annual National Conference on Cyber Security" is an annual program organized by Sri Lanka CERT since 2008, held in the month of October, which featured a series of events:

- Two Workshops for professionals, namely:
  - Virtualization Cloud Computing and Next Gen Enterprise Architecture
  - Network traffic analysis
- One-day Conference

d. Workshop on "End user security and cloud computing security" conducted jointly with ICASL.

4. Achievements

4.1 Publications & Other media

a. Website

The Sri Lanka CERT website publishes security related awareness bulletins for the public via News Alerts and a Knowledge Base. Glossaries, case studies and FAQs are among some of the other published items.

b. E-mails

Disseminating security related information via e-mail alerts to Sri Lanka CERT Website subscribers. The Cyber Guardian E-newsletter was initiated in mid-2011 and is distributed to a large number of students by the Ministry of Education, through the school net.

c. Newspapers/media

Sri Lanka CERT continues to educate the general public through the electronic and print media about emerging cyber security threats and vuln*erabilities.*

4.3 Certification & Membership

Memberships obtained in professional security organizations in the period 2010:

a. Microsoft SCP (Security Cooperation Program)
b. Collaborative agreement with "IMPACT". Sri Lanka CERT will benefit from receiving a threat feeds from the region and also form part of the global incident response team
c. Sri Lanka CERT is represented on the board and steering committee of the Information Systems Security Association (ISSA) Sri Lanka Chapter, and is involved in the planning of its inaugural event and strategic partnership formation efforts
d. Sri Lanka CERT is also actively supporting the formation of SLSEC, a proposed online forum where security enthusiasts can get help from fellow security enthusiasts. The forum will be managed by a governing body consisting of Sri Lankan representatives in Sri Lanka as well as overseas. The site will be hosted and managed, by Sri Lankan expatriates.

5. International Collaboration

5.1 MoU

In addition to being members of FIRST and APCERT, Sri Lanka CERT has signed Memoranda of Understanding with Microsoft, to be a member of Microsoft Security Cooperation Program (SCP) and with IMPACT, the security arm of ITU.

While a relationship with (ISC)² has also been established, Sri Lanka CERT will not enter into a Master Affiliate agreement with (ISC)². This is because the proposed business model is not financially viable. However, Sri Lanka CERT actively supported and has participation in the newly formed (ISC)² local chapter. It partnered with (ISC)² to run a CISSP boot camp as part of the CSW 2011 Program.

5.2 Event participation

March 22nd -25th, 2011
APCERT AGM & Conference
Jeju Island, Korea.

April 5th – 6th, 2011
Council of Europe International workshop
Sri Lanka

June 27th – 30th, 2011
FIRST AGM and Annual Conference
Vienna, Austria

July 1st – 2nd, 2011
National CSIRT Meeting

October 12th - 14th, 2011
FutureGov Summit 2011
Putrajaya, Malaysia

October 24th – 28th, 2011
UNAPICT - 2nd Regional Forum on ICT Capacity Building
Incheon, Korea

November 1st – 4th, 2011I

IMPACT Technical Training: Securing networks
Cyberjaya, Malaysia

5.3 International incident coordination

Active participant in the recently concluded APCERT Drill 2011, where Sri Lanka CERT played the role of Organizing Committee (OC) Lead and was part of the Exercise Control (EXCON) team.

Sri Lanka CERT has regular operational engagements with CERTs (US-CERT) and commercial organizations (such as Facebook, Google, Yahoo) to handle phishing, identity theft incidents.

6. Future Plans

6.1 Future projects

The following projects are either in the conceptual stage or just being initiated, and are intended to serve the constituency directly;

a. Development and Implementation of the National Certificate Authority
b. Implementation of the Telco CSIRT
c. Development and implementation of the Defense CSIRT
d. Conceptualization, development and implementation of the Edu-CSIRT
e. Cyber Security Week 2012

6.2 Framework

6.2.1 Future Operations

This section details the changes anticipated in Sri Lanka CERT with regard to staff, equipment and capabilities:

a. Commissioning of the Automated Incident Management System Tool; apart from speeding up the triaging process, this tool will also allow on the fly

maintenance of incident statistics.

b. Development, implementation and commissioning of the Automated threat analysis and visualization tool in conjunction with SLIIT
c. Re-designation of staff to allow one staff member to be the lead in a particular activity areas while understudying/assisting in another area (e.g. consultant – Network Security)
d. Introduction of virtualization technology at GIDC in conjunction with the NOC to allow migration of Sri Lanka CERT web server to GIDC servers, resulting in appreciable cost savings
e. Procurement of Qualysguard or equivalent automated penetration testing appliance to help speed up the automated scanning and reporting part of a penetration testing engagement, so human resources can be dedicated to manual verification purposes

6.2.2 Operational Support Projects

Sri Lanka CERT continues to maintain a sensor for the JPCERT/CC hosted TSUBAME InterneT Scan Data Acquisition System project, while collaborating with the Dragon Research Group (DRG) based in Brazil to deploy a sensor pod to collect and monitor data to identifying emerging threats. Hardware is available and being prepared for deploying a third sensor with the Shadow Server sensor network. Discussions are ongoing with INTECO-CERT of Spain and Team Cymru to deploy sensors in their respective networks.

All this information, coupled with the Automated Threat Analysis and Visualization tool would allows Sri Lanka CERT to spot developing incidents at a glance and proceed to take remedial measures.

7. Conclusion

Being nearly six years old, Sri Lanka CERT has faced an uphill task of raising Information Security awareness in Sri Lanka. The increase in the number of incidents reported and handled by Sri Lanka CERT in consecutive years is a

testament to the success of Sri Lanka CERT's awareness campaigns both through the use of seminars and conferences and through the use of popular media.

During this year most of the incidents reported to Sri Lanka CERT were related to phishing sites and various activities conducted through social networking sites, such as account hijacking and fake account creation. These were typically motivated by revenge, extortion or malicious software distribution.

All the events organized by Sri Lanka CERT during the year 2011 were very successful. We will continue to conduct the Annual National Conference on Cyber Security while finding new ways to reach an even wider audience, and also maintain a calendar of regularly running technical and management training workshops.

During the year, Sri Lanka CERT made valuable contributions to several APCERT working groups and helped to conduct a member survey, where Sri Lanka CERT was afforded the opportunity to analyze the data collected from the APCERT member survey 2011 and produce a report to the Steering Committee.

Sri Lanka CERT shall continue to participate in regional events such as the Annual APCERT drill and also welcomes opportunities to collaborate with its sister CERTs in incident coordination.

We look forward to being a bigger part of APCERT in 2012 by contributing to various working groups and activities in order to build a secure information environment in the Asia Pacific region.

14. ThaiCERT Activity Report

Thai Computer Emergency Response Team– Thailand

About ThaiCERT

Responding to computer security's incidents is the main mission of ThaiCERT. ThaiCERT has been receiving a number of security incident reports since the year 2001 – the year of ThaiCERT establishment - and coordinated with related entities to obtain a satisfied resolution for the reported incidents. In the beginning, ThaiCERT only provided computer security response service to Thai government units, but since the emerging of various security incidents which arose in Thai Internet community the service was expanded to private organizations in order to coordinate the closing of their compromised cases.

In February 2011, by the resolution of Thai cabinet, ThaiCERT operations were transferred to a new administrative team in a new public organization named Electronic Transactions Development Agency (ETDA), under the supervision of Ministry of Information and Communication Technology. However, this organizational restructuring had not affected the objective of ThaiCERT, which has been and continues to be a national and not-for-profit CSIRT. Her main role still remains to be an official point of contact for dealing with computer security incidents in Thai Internet community. After the process of re-establishment has ended, the new ThaiCERT was back in service from July 2011. This annual report contains information of ThaiCERT organization, reported incident statistics and activities under ETDA between July to December 2011.

Constituency

ThaiCERT's constituents were Thai Internet users including those in public, private and home sectors. In addition, ThaiCERT provided her incident coordination service to other international entities, where the sources of attacks were originated within Thailand.

Staffing

ThaiCERT currently employs 8 full-time staff consisting of 1 executive director, 1 head of operation, 1 security specialist and 5 computer engineers.

Certification

ThaiCERT's staff were holding the following professional security certificates

- ISC² CISSP
- IRCA ISO/IEC 27001 ISMS Lead Auditor
- CompTia Security+

Reported Incident Statistics

ThaiCERT classified the reported incidents according to ECSIRT incident classification[1] for the purpose of collecting statistical data. In general, a security incident can have multiple incident types and a security incident can be reported by multiple parties. To avoid the duplication of incident counts, a reported incident was counted only in its incident type based on the type of incident coordination request. For example, after a computer was compromised, an attacker used the computer for a phishing. As a result, the incident has multiple incident types, which are intrusion and fraud. When the incident was reported to ThaiCERT, only one incident was counted up with only one incident type. If the reporter requested a coordination service to resolve the intrusion incident, the incident was counted as an intrusion type. On the other hand, if the reporter requested to obtain the resolution to taking down the phishing page, the incident was counted up in a fraud type. Also, it is possible that the same incident was reported by multiple entities, but all the duplicate reports were counted as only one incident.

[1] ECSIRT Incident Classification - http://www.ecsirt.net/cec/service/documents/wp4-clearinghouse-policy-v12.html#HEAD6

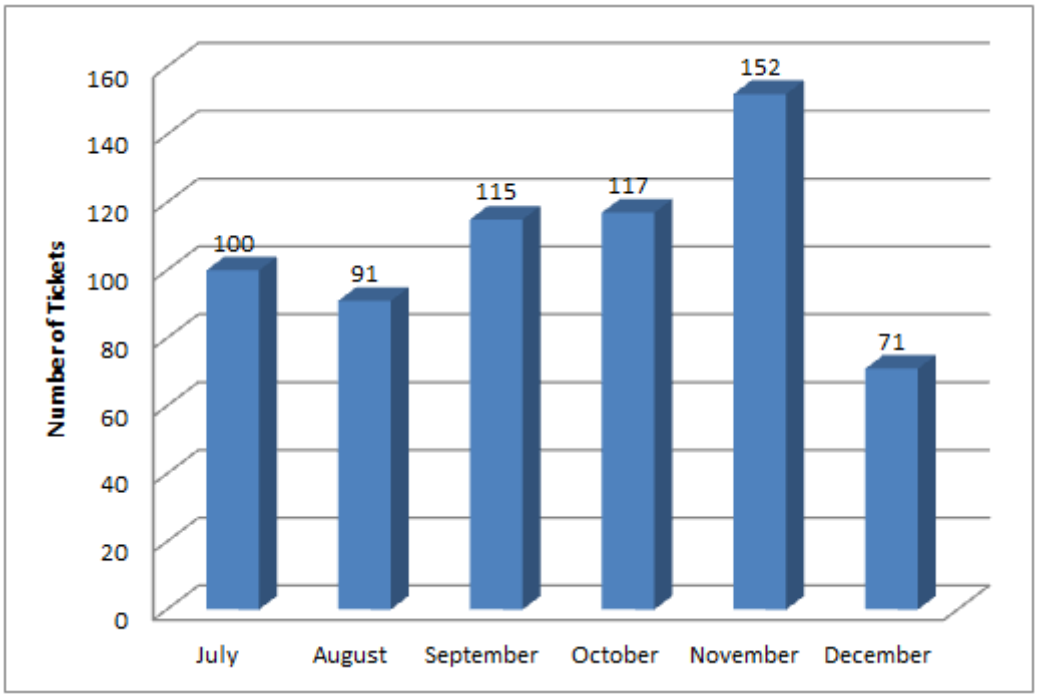


Figure 1 The number of reported incidents by month between July and December 2011

As can be seen in Figure 1, the number of reported cases ("ticket") had been on the rise with an average more than 100 tickets per month since the restructuring of ThaiCERT in July 2011. However, the number of tickets suddenly dropped in December because of the discontinuity of the old ThaiCERT email with NECTEC's domain (thaicert@nectec.or.th), and this was because a number of reporters still used ThaiCERT old email for incident reporting. After the re-notification of the new ThaiCERT email for computer security incident report (report@thaicert.or.th) to the public, we expect to see the ticket numbers resume their rising trend and continue to increase in year 2012.

Figure 2 shows the proportion of reported incident types to ThaiCERT in year 2011 between July and December. As can be seen from the figure, the top 5 types of reported incidents contribute to 98% of all reported cases, and these include Fraud, Intrusion Attempts, Information gathering, Abusive content and Malicious Code, consecutively. The top reported incident type was fraud, with 47.8% of the pie and all of them were phishing cases. The 2nd and 3rd top reported cases were in

intrusion attempts and information gathering types, with 14.6% and 14.4% of the pie. These attacking or security scanning cases were mostly on the standard remote access TCP/UDP ports, especially SSH brute-forcing and FTP brute-forcing. Abusive content was the top 4th type in the rank, with 11.9% and all of them were reporting on spambots or machines sent spam. Note that the Spam-related incident was the top most frequent reported incident to ThaiCERT in 2010[2]. The incident type related to malicious code was the last in the top 5, with 11.9%.

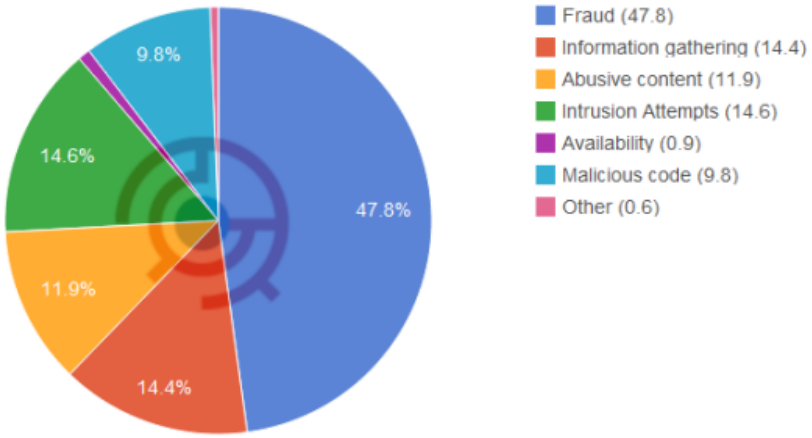


Figure 2 The proportion of incident types of reported cases, between July and December 2011

[2] APCERT Annual Report 2010

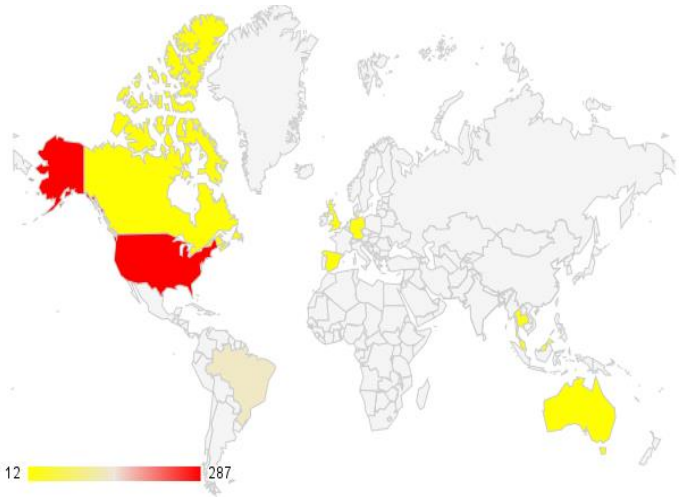


Figure 3. The top reported incidents to ThaiCERT by country

As illustrated in figure 3, the most frequent country reporting the incidents to ThaiCERT was obviously United States, with 44.42% of all cases. The next most frequent countries were Brazil with 21.05%, Thailand with 4.33%, Malaysia with 3.72%, Singapore with 3.72%, and Germany with 3.56%. The rest 19.20% were reporting security incidents from countries reporting the incidents less than 12 tickets or an average less than 2 tickets per month.

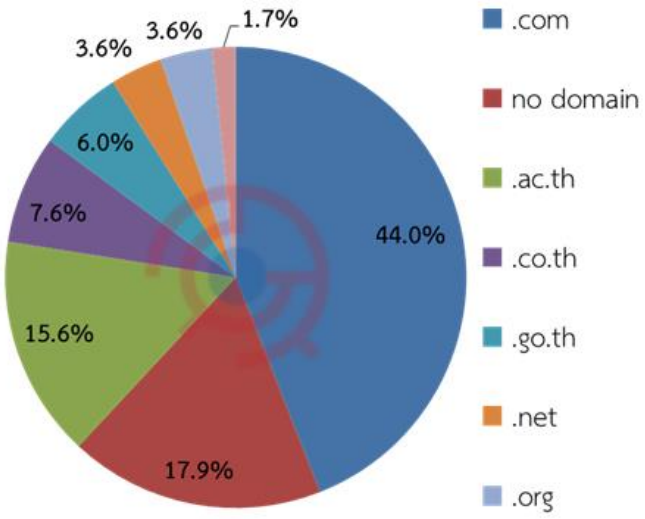


Figure 4 The proportion of reported phishing domains on Thai Hosts in 2011

Phishing Statistics

There were totally 302 reported phishing cases on Thai hosts in 2011, and these phishing cases were found on 165 Thai hosts. Clearly, we observed that some reported hosts were hacked or compromised multiple times to host phishing sites. Figure 4 shows the distribution of reported phishing domains on Thai hosts in 2011. The top most reported phishing domain was generic commercial top-level domain (.com) and it contained 44.0%. The 2nd largest portion of reported phishing (17.9%) was reported by IP addresses and these addresses could not be reverse resolved to a domain name. 15.6% of all reported phishing were found in Thai academic domain (.ac.th). Phishing in Thai commercial domain (.co.th) was 7.6% of all reported phishing cases and followed by phishing in Thai government domain (.go.th) with 6.0%. Interestingly, the reported phishing domains shown above were different from Global Phishing Survey: Trends and Domain Name Use in 1H2011 report, in which APWG said that most phishing in Thailand took place in academic and government web servers.

Alerts and Advisories

ThaiCERT provided technical information on computer security, attacking trend and security incident statistics, and also published technical advisories on vulnerability that may cause a major impact on Thai's Internet community. All publications were published in Thai language and available on ThaiCERT's website (www.thaicert.or.th).

Activities

Events organized or participated

- In August 2011, ThaiCERT organized a government drill with participation from Thai Ministries and major telecommunication operators. The objective of the drill was to introduce the incident response framework and promote the incident coordination process among the government organizations, and the theme of the drill was "handling web defacement and phishing"
- ThaiCERT successfully participated in ASEAN CERTs Incident Drill

(ACID 2011) hosted by SingCERT held in September 2011

- ThaiCERT and JPCERT/cc co-organized an advanced security training on the topic "Secure C/C++ Programming" in Bangkok held in May 2011

Conferences/Events/Trainings

In 2011, ThaiCERT participated in a number of both local and international conferences, including:

- Attended APCERT AGM & Conference 2011, Jeju, Korea, March 2011
- Attended FIRST Annual Conference 2011, Vienna, Austria, June 2011
- Attended Apectel DNSSEC training hosted by MCMC, Kuala Lumper, September 2011
- Invited to give a talk at National Cyber Security Conference 2011 (NCSC 2011), organized by Ministry of Defense, Bangkok Thailand, October 2011
- Invited to give a talk at ITU/ASEAN Subregional CSIRT/CIRT/CERT Workshop for CLMV, Rangoog, Burma, November 2011
- Invited to give a talk and be a chair of conference sessions at 2nd APT Cybersecurity Forum, Tokyo, Japan, December 2011

15. TWCERT/CC Activity Report

Taiwan Computer Emergency Response Team / Coordination Center – Chinese Taipei

1. About TWCERT/CC

1.1 Introduction

Taiwan Computer Emergency Response Team / Coordination Center (TWCERT/CC) is a security organization for computer intrusion handling, security-related resource and tools providing, latest vulnerability information publishing, and security education popularizing. In addition to play a coordination role in Taiwan security domain (.tw), TWCERT/CC actively participates in international network security organizations and actions to strengthen communication and coordination with CERTs. Expect to provide users with a safe and convenient internet environment under cooperating with domestic and international security organizations.

1.1.1 Establishment

TWCERT/CC formally established since 1998. The major purposes of TWCERT/CC are to prevent and actively assist the computer and network security incidents in Taiwan, to analyze the system vulnerabilities, to provide computer and network security tools and related documents for the system administrators and the programming guidelines for the developers, and conduct a series of training programs to raise the awareness of network security. TWCERT/CC is constantly reinforcing the organization functions and refining the network security services. With the dedicated devotion and seamless collaboration of the whole team, TWCERT/CC has accomplished several significant gradational goals and missions as follows:

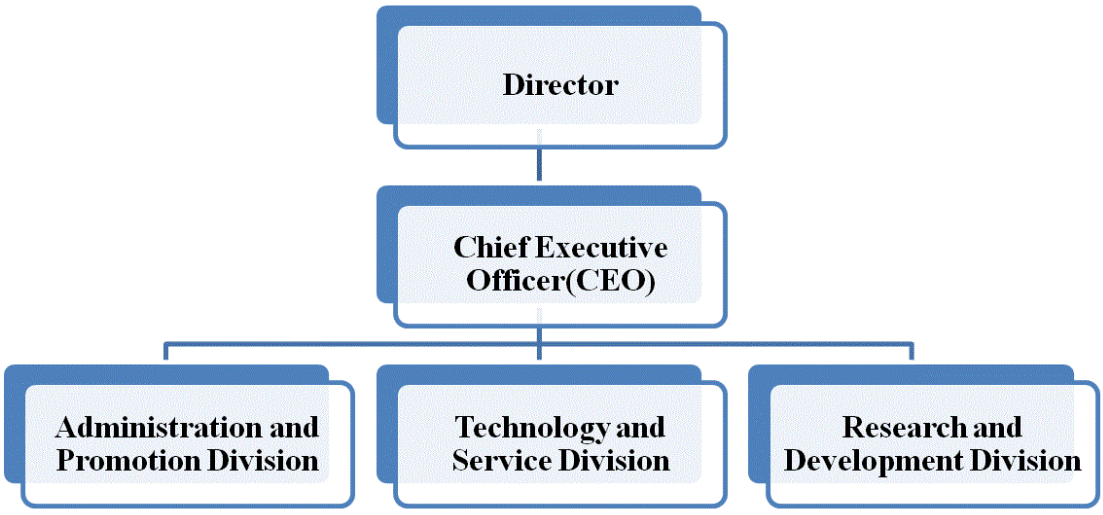
(1) To assist the handling of the intrusion incidents in the constituency, .tw domain.
(2) To announce the system vulnerability information.

(3) To provide security training and education on protection and defending technologies and skills.
(4) To assess periodically the national-wide security level in the Internet.
(5) To be the point of contact of Taiwan for international coordination.

The main purpose of TWCERT/CC is to provide assistance to handle the incidents regarding information and network security. By raising the security awareness in our network community and developing security technologies to improve the liability of the network environment. Our missions are:

- Speed up the circulation of network security information to enhance the safety of domestic information and networks.
- Research and develop the computer network detecting and defending skills to strengthen the network safety.
- Facilitate the foundation of each organization's emergency response team, promote the national wide network security, and reconcile the combination and interchange on security information.
- Encourage and coordinate the exchanges and cooperation between each international emergency response institution to maintain the global network security.

1.1.2 Organization



2. Activities & Operations

2.1 Incident Report Handling

Frequent incidents show that it is great urgent to improve system and network security. To defend hacker intrusion and stop up security threats spreading, TWCERT/CC works hard for safeguarding security and plays the contact agent for sharing the experiences on dealing Taiwan's network security incidents with other CERTs. Expect to achieve the following goals:

Year	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011
Total	962	1260	5318	2874	1824	788	660	1087	679	1094	6666

Table 1. TWCERT/CC incident response statistics

(1) Possible incidents prevention: provide an incident response channel and the prevent mechanism for the victims to avoid analogous events happening.

(2) Real-time Incidents handling: offer an immediate warning and defense force to effectively restrain and control incidents extending.

(3) Recovery support: provide technological consultant and support to recovery operation and reduce damage.

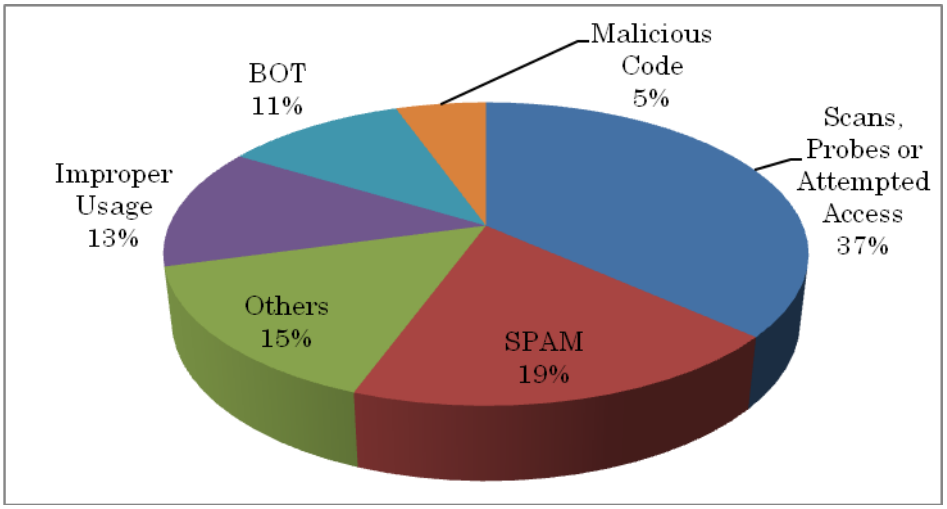


Figure 1 TWCERT/CC incident response classification statistics

■ **Security Vulnerability Announcement**

To promote system and network security and reduce damage from intrusion, TWCERT/CC is devoted to strengthen services, to publish latest security issues, to provide security documents/tools, vulnerability patch information and security related documents download, and actively research attack/defense technologies.

Year	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011
Advisory	172	258	142	197	140	138	119	49	44	234	98

Table 2. TWCERT/CC advisory statistics

■ **Mailing List and Newsletter Service**

TWCERT/CC has collected and compiled security documentations and the advisories from various foreign hardware and software companies. The information has been evaluated and translated into the localized language, the staff dispatches to the Taiwan publicity to achieve the synchronicity of worldwide circulating information as soon as possible. In addition, the monthly TWCERT/CC Newsletters include special columns on the latest network security information and technologies that can raise the network security awareness in Taiwan.

■ **Information Security News Update**

TWCERT/CC researches, analyzes and develops technology and training aimed at helping administrators to secure their systems and networks. TWCERT/CC irregularly provides security related information, such as security tools, advisory, vulnerability remediation, technology documents, for the multitude and security-conscious users to enhance security education and consciousness.

■ **Localized Vulnerability Database**

The major purpose of the establishment of the localized Vulnerability Database is to collect the information of software vulnerabilities and system weaknesses. The vulnerability database contains 49 categories and up to 29 thousands records. We will continuously invest manpower to maintain and update. The major categories are shown in Fig. 3.

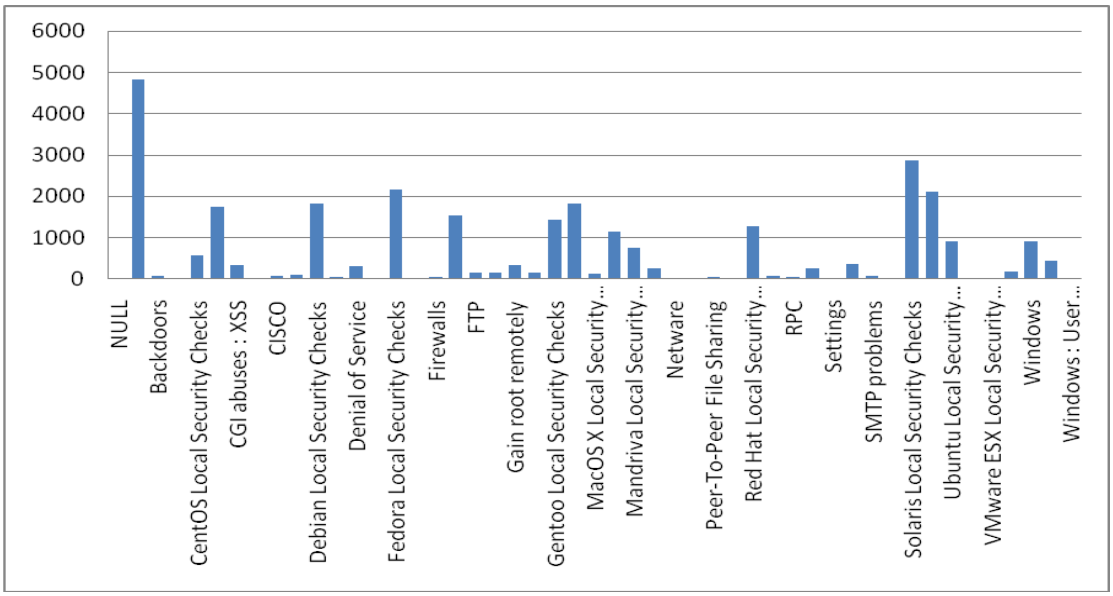


Figure 2. Categories of TWCERT/CC Vulnerability Database

■ **Information Security Training**

TWCERT/CC provides a series of security training/education for government agencies and industries to enhance and enrich their knowledge and capability on network and information security. The training course also gives people a channel to exchange information and hands-on practice related to security. By adopting e-learning, TWCERT/CC education courses feature a synchronous/asynchronous on-line learning, a flexible study schedule, and independence learning without time/space restriction to accommodation the different needs of the learners.

■ **Member Services**

TWCERT/CC offers products, service and resources to help registered members find the best approach to security and continuously researching various aspects of computer security to benefit our members.

2.2 Abuse statistics

■ **Spam analysis report**

TWCERT/CC statistics and analysis of spam regularly, collects 502,012,632 total from May 1, 2011 to December 31, 2011. The countries which the spam come from

up to 144, the first one is Asia for 87%.

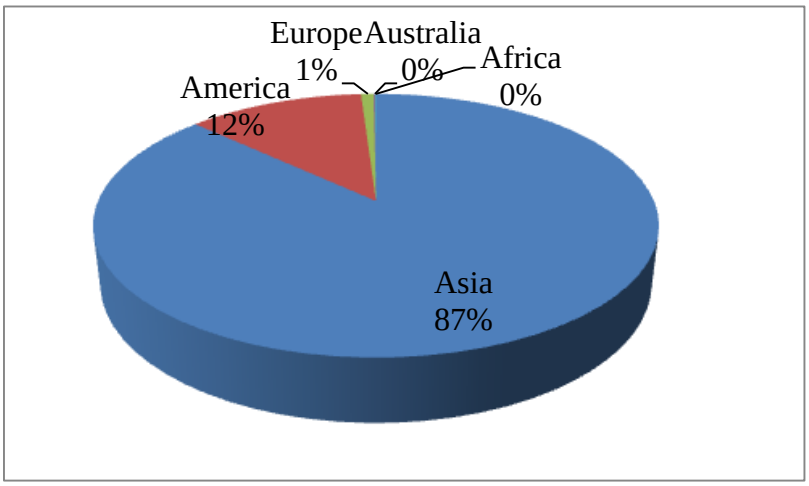
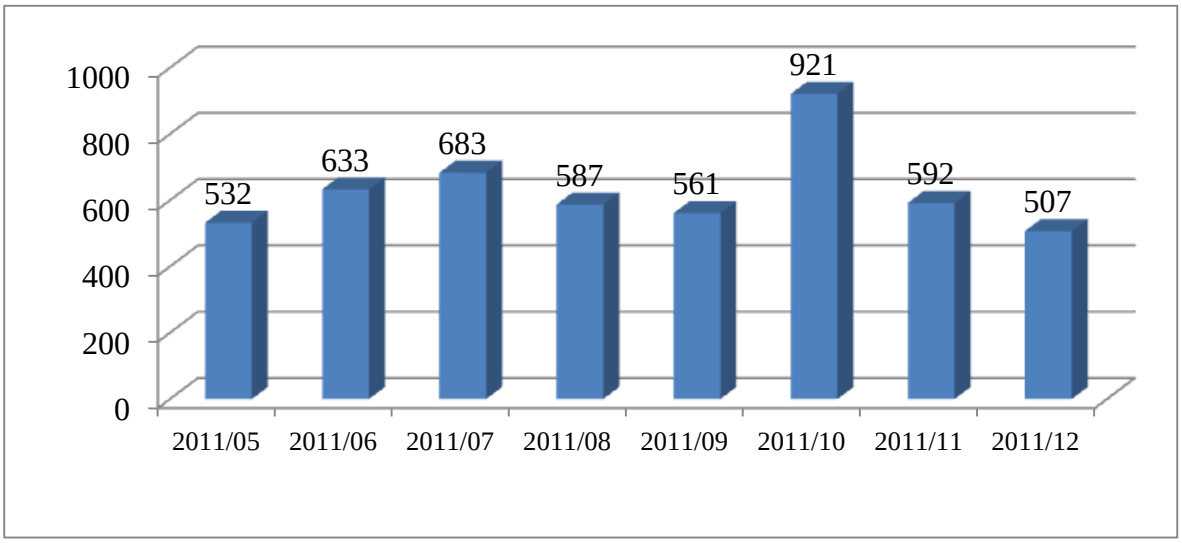


Figure 3 Ratio of the source of spam



Unit：Ten Thousand

2.3 New Services

■ **Anti-Phishing Notification Window**

TWCERT/CC provides the Anti-Phishing Notification Window for Phishing incident notification. When people discovered that there is Phishing Web Site or Company Web Site is injected phishing page, notice these via this window. TWCERT/CC would inform ISP/involved units of phishing incident to avoid expanding. The

Anti-Phishing Notification Window：
http://www.apnow.tw/index.cgi

3. Events organized / co-organized

3.1 Information Security Training

TWCERT/CC hosts seminars or training regularly to popularize network security knowledge, to enhance system administrators' skills, and provides a good interaction channel for personal training and education promotion.

Date	Subject
2011/11/11	Network Traffic Analysis
2011/10/13	Cloud Security Technology
2011/9/16	Windows Rootkits Detection
2011/8/25-26	The analysis of Malicious code and Digital Forensic
2011/8/5	Web Application Security
2011/7/15	Windows Rootkits Detection
2011/7/13	DNS Security
2011/6/17	Linux Virtual Server
2011/6/3	Cloud Security Technology
2011/5/16	Linux Network/Server Security
2011/5/13	Establishing a Honeynet
2011/5/6	DDOS Attacks and Defense
2011/4/20	The analysis of Malicious code and Digital Forensic
2011/4/15	Web Application Security
2011/3/11	DNSSEC – Linux /BIND
2011/2/8	Intrusion Detection and Prevention

Table 3. Timetable of TWCERT/CC Training

3.2 Drill

TWCERT/CC helps TANet(Taiwan Academic Network) to run Information Security

informative drill program during a period of two weeks, a total of 4,094 educational institutions involved in this successful program and the completion rate is 99%.

4. Achievements

The government and organizations recently pay much attention to information and communication security promotion and development. TWCERT/CC has made great efforts to manage in security field many years for enhancing network safeguard to protect against the increasing intrusion and attack.

- **Enhance domestic network security**

The main purpose of TWCERT/CC is to provide assistance to handle the incidents regarding information and network security. By raising the attention of network community to security issues and conducting the research on computer systems, we manage to enhance the fail-safe systems of computers and networks, and proceed to prevent the incident before hand. We disseminate system vulnerability information to raise the awareness of network security, identify and resolve the system vulnerabilities on various platforms, and work with security researchers to develop the prevention and protection techniques to improve the network security.

- **Encourage and coordinate incident response**

TWCERT/CC is devoted to promote collaborative research and development on cyber security to reduce the loss caused from incidents. TWCERT/CC plays a major communication agent for encourage and coordinating the exchanges and cooperation with domestic ISPs and international CERTs or CSIRTs to maintain global network security.

- **Security promotion**

TWCERT/CC works to create an international workforce skilled in information assurance and survivability by developing curricula and training for executives, managers, engineers, network administrators and operators. Furthermore, TWCERT/CC held seminars and education training programs to promote the

importance of security awareness and to enhance the ability of security administrators in a proactive way. Such interactively training provides a great channel for information sharing as well as skill improvement.

- **Security training**

Recently frequent incidents encourage security awareness and professional demand. Personal training is the major work in technology development. TWCERT/CC offers many introductory and advanced training for executive, managers, educators, engineers, cyber administrators/operators and so on. TWCERT/CC has trained many good talent of security field who are responsible for the security of information assets in different organizations. Hope to enhance domestic research and development capacity by mutual support and cooperation.

- **International relationship**

TWCERT/CC actively participates in international organizations and activities, and improves our capabilities and services. We have joined in FIRST, APCERT and Anti-spam MoU to be the international coordination in Taiwan to reinforce the information exchange and collaborations among all the other CERTs around the world. On account of the cooperation among the network security organizations, we expect to provide a secure and convenient network environment for the Internet users.

4.2 Publication

Each month, TWCERT/CC issues Information Security E-News to provide Information Security notice, activity, and News summary in that month. TWCERT/CC also invites domestic experts/scholars to write a monthly Information Security column and special report, assist user in learning information security news/tech, improving security of the network usage.

4.3 Certification

Staff hold the following certificates.

- ISO 27001 Lead Auditor

- ISO 20000 Lead Auditor
- Certified Ethical Hacker

5. International Collaboration

In addition to make efforts in security improvement in our domain, TWCERT/CC actively participates in the international security organizations and actions to enhance communication and cooperation. TWCERT/CC played a major communication agent for encouraging and coordinating the exchanges and cooperation with the international emergency response institutions to maintain the global network security.

- To participate in international forums and meetings, to exchange the related security intelligence with each emergency response center.
- To form a transnational defense system to handle international incidents.

Forum of Incident Response and Security Teams (FIRST)

FIRST is the Forum of Incident Response and Security Teams. It was clear from then on that information exchange and cooperation on issues of mutual interest like new vulnerabilities or wide ranging attacks - especially on core system like the DNS servers or the Internet as a critical infrastructure itself - were the key issues for security and incident response teams. FIRST brings together a wide variety of security and incident response teams including especially product security teams from the government, commercial, and academic sectors.

TWCERT/CC becomes the first official international coordination in Taiwan by joining the FIRST in October 2001 to share the latest security information and technologies in FIRST forum with members, attends annual FIRT conference to establish a transnational security joint defense system and enhances incident-handling capability for integrated early-warning mechanism.

Asia Pacific Computer Emergency Response Team (APCERT)

Besides globalization organizations, Asia Pacific Computer Emergency Response Team is a regional coordination organization established by countries of the Asia

Pacific region in 2002 to enhance regional and international cooperation on cyber security. APCERT cooperates with CERTs and CSIRTs to maintain a trusted contact network of security experts in the Asia Pacific region to improve the region's awareness and competency in relation to cyber security incidents.

TWCERT/CC jointly develops measures to deal with large-scale security incidents and phishing attack, and exchange technologies and experiences with APCERT members to manifest Taiwan much effort in security and help to understand the latest development and tendency in the Asia Pacific region.

- **Seoul-Melbourne Multilateral Memorandum of Understanding on Cooperation in Counting SPAM**

E-mail becomes a major application with the population of computer and network, however, the following spam abuse is getting more and more rampant. Spam not only wastes individual and enterprise cost, but also endangers information and network security. Enterprises and the government have to face and restrain the spam threat which is a global authorized problem. In addition to legislation and management, the most important is to set up a transnational and trans-organizational cooperation to effectively stop spam persecution.

Seoul-Melbourne Multilateral Memorandum of Understanding on Cooperation in Counting SPAM is an agreement signed by Australian Communications and Media Authority (ACMA) and Korea Information Security Agency (KISA) in 2003. Participates in Seoul-Melbourne MoU are part of a network of computer security incident response and security teams that work together voluntarily to deal with spam problem and prevention.

TWCERT/CC has been promoting the training of computer-network security response for years. Since 2005, TWCERT/CC has officially joined Seoul-Melbourne MoU member, and played the contact agent for sharing the experiences on dealing Taiwan's spam issues and exchange the anti-spam jurisdiction process with other members.

The key points of our missions are:

- To cope Taiwan's network security incidents with other nations, and take the part as a coordination center;
- To assist in handling the transnational spam problems;
- To exchange the related security intelligence with each member;
- To participate in international forums and meetings related to network security, and to uplift Taiwan's international image and position.

6. Future work and Conclusion

In order to improve the international involvement, TWCERT wishes to participate in transnational incident investigation and response assistance and to enhance Taiwan's visibility. As the personal privacy legislation is going to be effective soon, different sectors put more attention on security. Beside international coordination, horizontal collaboration on incident response is essential, too. Government organized CIIP (Critical Information Infrastructure Protection) drill initiates collaboration among different agencies and organizations. The future work will emphasize the harmonic and efficiency of the coordination among different levels and across the nation.

- Work for security related research and development to advance the international visibility.
- Participate in international interchange and coordination to form a transnational joint defense mechanism.
- Jointly developing measures to world-scale network security incidents and know well the international security tendency and development to advance global internet environment.
- Train the awareness and capability in information security and risk management through information sharing and international cooperation.

16. TWNCERT Activity Report

Taiwan National Computer Emergency Response Team – Chinese Taipei

1. About TWNCERT

TWNCERT (Taiwan National CERT) was built in 2001 and as known as ICST (Information & Communication Security Technology Center) domestically is the leading CSIRT in Taiwan public sector. TWNCERT is intended for improving incident response and information security awareness and sharing in Taiwan. It is mainly dedicated to create a response center that can help optimize the capability of real-time monitoring, coordination, response and handing in the face of security incidents.

The missions of TWNCERT include:

- To coordinate among relevant agencies and organizations to identify pertinent response and actions in case of security incident.
- Providing an information analysis and exchange center for information at home and abroad.
- To help relevant government agencies to set up computer emergency response team (CERT).
- To provide government agencies reference information for formulation of security policies.

TWNCERT services including:

- Alert and publication: Guarding against and publishing probable security threats (e.g. vulnerability analysis).

- Technical service: Providing technical service to government agencies.

- Assistance in the setup of CERT: Assisting interested agencies to set up their own CERT.

- Consultation: Making suggestions regarding operation and R&D of computer security and Internet issues.

- Strategy recommendation: Making suggestion to government agencies regarding strategic planning.

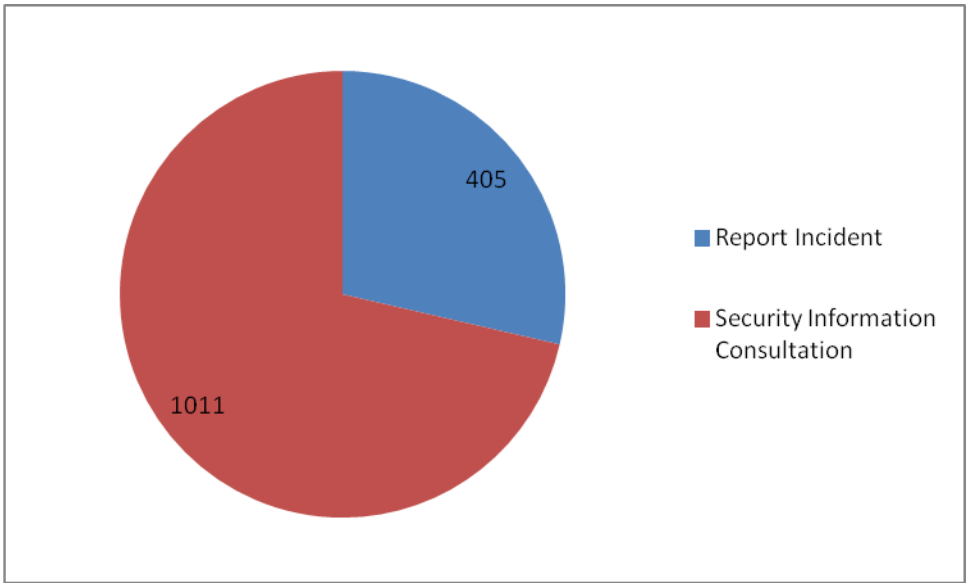
- Risk analysis: Undertaking risk assessment.

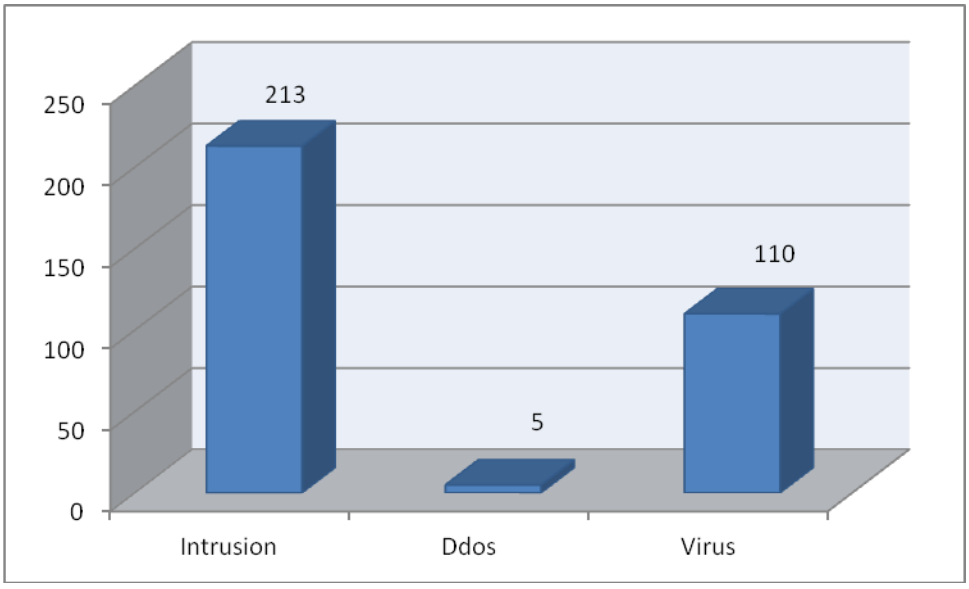
- Collaboration: Building collaborative relationship with legal community, information security business and ISP.

- Coordination: Building coordination and communication channels with domestic and foreign incident response organizations.

2. Operations & Activities

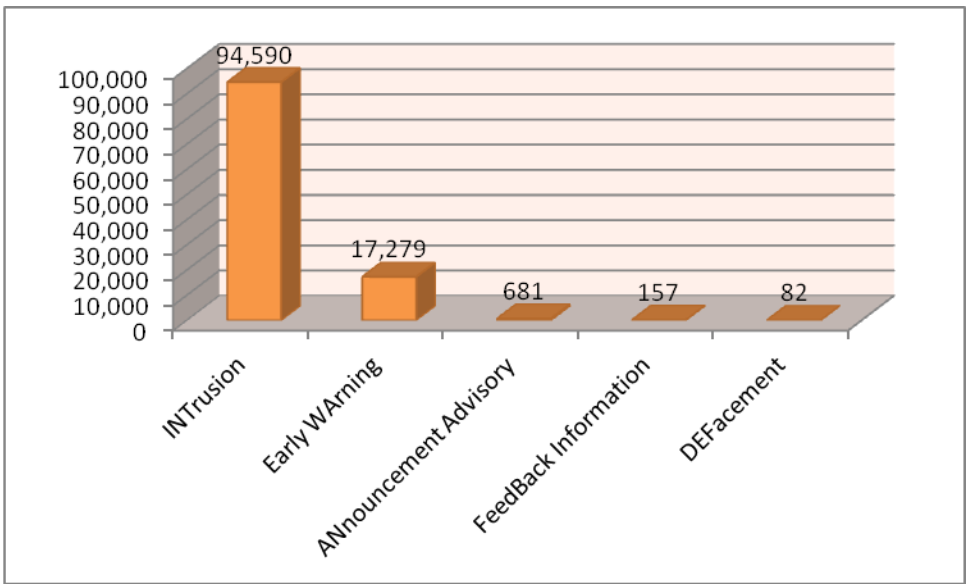
- In 2011, TWNCERT received 405 reports on computer information security incidents from Taiwan government sectors, the top 3 incident categories are Intrusion, DDoS and virus. TWNCERT also offers 1,021information security consulting service.



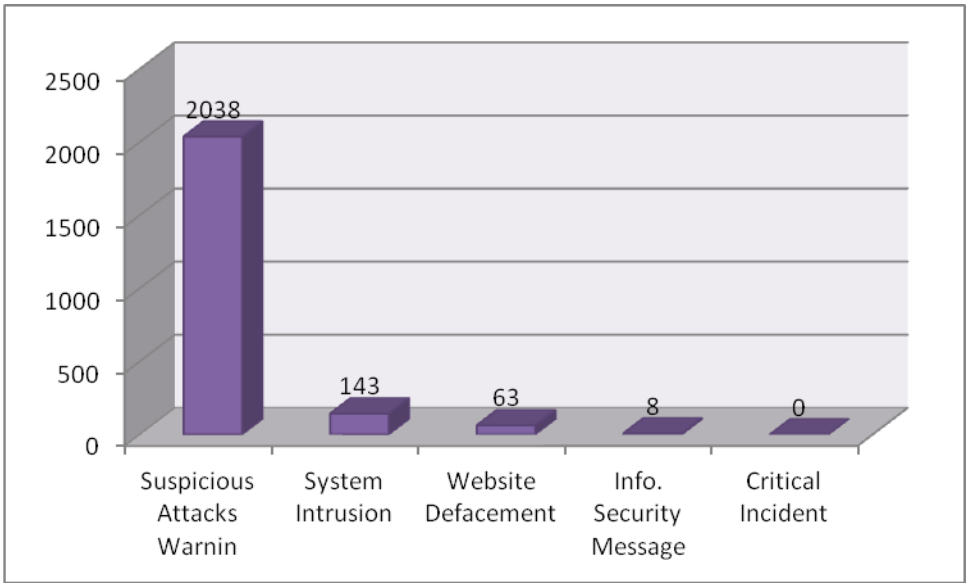


- Since 2011, TWNCERT started running a government ISAC, called G-ISAC (Government Information Sharing and Analysis Center). TWNCERT began not only deal with government sectors information security relevant, but also sharing security information with Academic ISAC(A-ISAC), National Communications Commotion ISAC(NCC-ISAC) which has 6 major ISPs. In addition, TWNCERT has major SOCs, CERTs such as TWCERT/CC and EC-CERT (Electronic Commerce CERT) as G-ISAC members. G-ISAC is

using IODEF format and secure API system to make sure the information is useful and in time and based on a trust membership. Currently G-ISAC is cover 99.4% IPS in Taiwan and have sharing over thousand security incident or critical information. G-ISAC members shared totally 112,789 information in 2011.

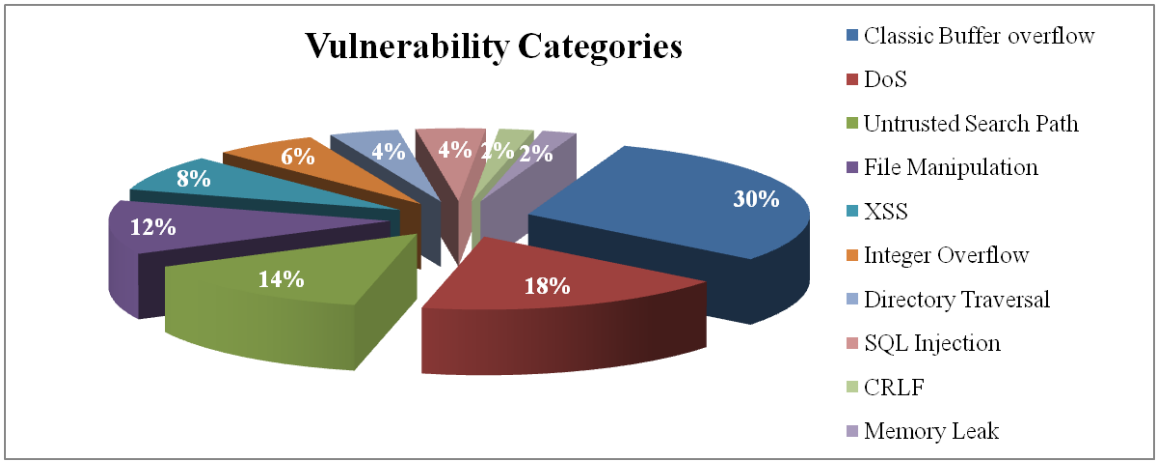


- In 2011, TWNCERT published totally 2,252 advisories, including:
  - Suspicious Attacks Warning: 2038
  - System Intrusion: 143
  - Website Defacement: 63
  - Info. Security Message: 8
  - Critical Incident: 0



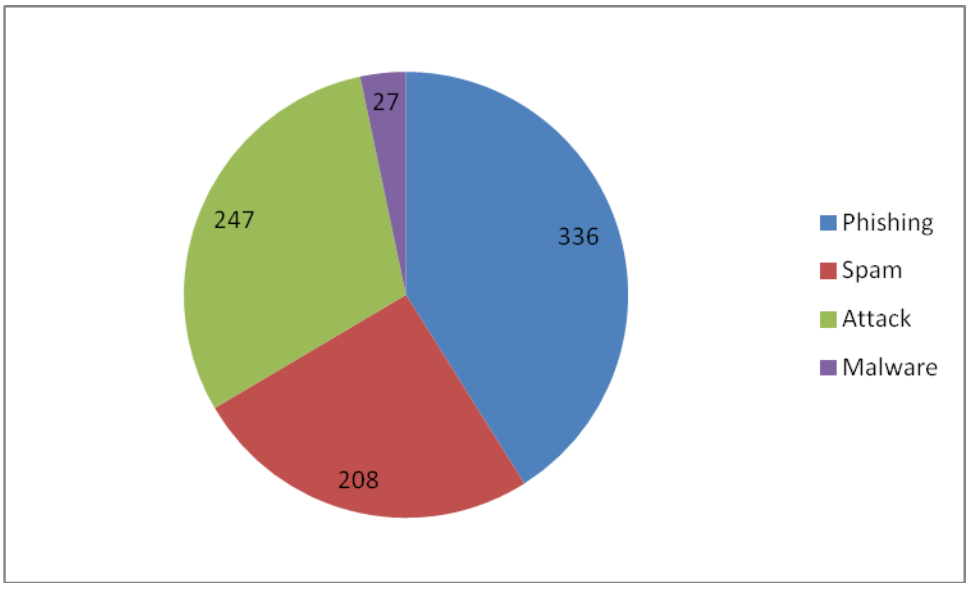
3. Achievements

- Since 2011/5, TWNCERT has first-found 50 SCADA exploitable and got 25 CVE Identifier number:
  - CVE-2011-1914、CVE-2011-3330、CVE-2011-3996、CVE-2011-4033、CVE-2011-4034、CVE-2011-4035、CVE-2011-4036、CVE-2011-4043、CVE-2011-4053、CVE-2011-4055、CVE-2011-4056、CVE-2011-4057、CVE-2011-4521、CVE-2011-4522、CVE-2011-4523、CVE-2011-4524、CVE-2011-4525、CVE-2011-4526、CVE-2011-4533、CVE-2011-4534、CVE-2011-4870、CVE-2012-022、CVE-2012-023、CVE-2012-0309、CVE-2012-0310



4. International Collaboration

- Attended FIRST 2011 in June 211
- Attended Blackhat USA in July 2011
- Attended APEC TEL 44 in September 2011
- Attended AVAR 2011 in November 2011
- Attended the 10th RAISE in November 2011
- In 2011, TWNCERT totally received more than 827 international information security incident reports. Assisted and cooperated with other CSIRTs and governments.



- Reporting Botnet Incidents to 14 countries. Includes Netherlands, Germany, France, USA, Indonesia, Australia, Singapore, South Korea and Japan.

17. VNCERT Activity Report

Vietnam Computer Emergency Response Team – Vietnam

1. About VNCERT

1.1 Introduction

VNCERT is an agency under Ministry of Information and Communications of Vietnam, established by decision of Vietnam's Prime minister in December, 2005. In Vietnam, VNCERT is responsible for state management of information security area.

Roles of VNCERT:

- Coordinating national computer incident response activities.
- Watching and warning computer network security problems.
- Building and co-ordinating to build computer network security technical standard.
- Promoting to build CERTs in the organizations, enterprises, and agencies in Vietnam.
- VNCERT is the point of contact of Vietnam with the oversea CERTs in this area.
- Support Ministry of Information and Communications with activities in state management about Information Security.
- Lead the process of deploy the Anti-spam Law (Decree No.90 of the year 2008) in Vietnam.

1.2 Staff and structure

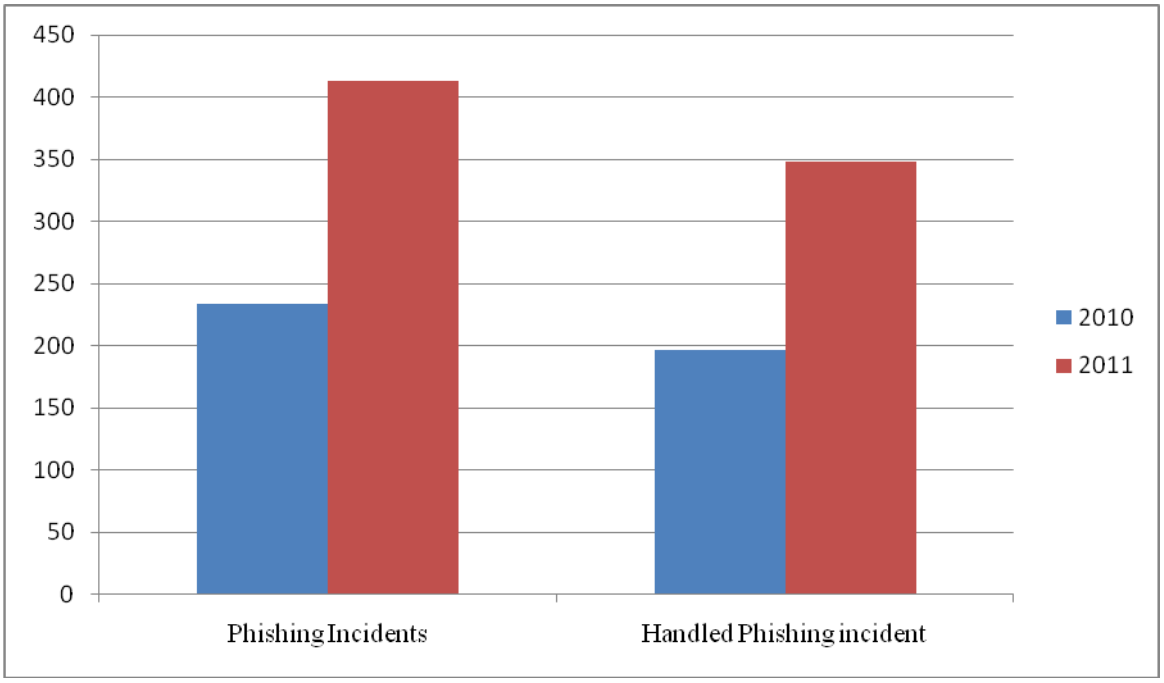
VNCERT has four specialized divisions: Division of Operation, Division of System technique, Division of Training & Consultancy and Division of Research and Development. VNCERT also has two branches, one in Ho Chi Minh city and another in Da Nang city.

Current number of employees in VNCERT is about sixty.

2. Activities & Operations

2.1 Incident reports & handling

In 2011, the total number of incidents were reported to VNCERT was 732, in which 385 phishings, 334 defaces and 13 malwares. Some websites of Government and online newsspaper were DdoS attacked, seriously, a newspaper was under DdoS attacked during a month. Many reports were about phishing and malware as well as spam sources. Almost phishing cases were related to finance, commonly forging banks' website to steal bank's account, and they were reported from outside Vietnam.



Pic.: Phishing Incident Report on 2010, 2011.

2.2 Watching and supporting activities

VNCERT also actively watched security news from many sources, and warned about security threats to organizations via private channels or to Internet users via media press.

VNCERT has supported some state organizations and industries to audit critical information systems and enhance system security.

VNCERT helped to secure all online important government events.

2.3 Anti-spam activities

Published and deployed Decree 90/2008, Circular 12/2008, Circular 03/2009 to prevent spam messages.

VNCERT has issued nearly 100 certificates to Content Provider for providing advertising services on SMS, email and SMS over Internet.

2.4 Legal environment improvement

We are preparing to start a Cybesecurity Law project.

And VNCERT are preparing to submit to Government for a news Decree 90.2008/ND-CP.

We just launch a Ministry Decree about to building a nework of Incident Response Teams on Government organizers, ISP and voluteer organizers in Vietnam.

3. Events organized / Co-organized

3.1 Training & Drills

In 2011, VNCERT arranged some training courses for raising information security awareness as well as working experience in Information Security field to staff in some organizations and an expert training program in malware code analysis

VNCERT participated in 02 international drills: ASEAN CERTs Incident Drill (ACID 2011) and APCERT Annual Drill 2011.

VNCERT coordinated to organize Information Security contest between the students of universities in Vietnam.

3.2 Seminars & Etc

Co-operated with Ministry of Public Security and IDG Vietnam Corporation to organize annual event "Security World", the largest IT security conference in Vietnam. Security World Conference & Expo 2011 featuring on the main theme “Securing your Organiztions in a connected world” presents an ideal opportunity to connect with true peers – the top IT executives – CIOs, CSOs.

Co-operated with VNISA to organize successfully an conference related e-government and to organize the annual event "National Information Security Day 2011" with theme "Digital information security - the foundation of strong IT nations", the biggest and most important security conference of the year. The event was hosted by Ministry of Information and Communication to raise some extent the important role of information security nowadays

Co-organized the first CSO Conference & Awards, featuring the theme: "Information Security – Facing the threat", When security information is threatened by the attack with large scale and clear purposes, the solutions of security system of the organizations is becoming more urgent and essential than ever. Therefore, CSO – the leaders of information security and their contributions are vital.

3.3 Consultancy

VNCERT supported the state and private organizations in the IS area and helped the Government to develop the national strategy to secure cyber-space.

Besides, VNCERT provided assessment service to government agencies, bank and enterprises, helped them in auditing their system and procedures. To organise to train couses to them about information security.

Organize the training programs to guideline implementing new legal documents.

4. Achievements

Took part in the national and international conferences related IS hosted by ITU, APECTEL, MERIDIAN and others.

Support to Government agencies to react with Big DDoS incident and require ISPs to block malicious servers on abroad.

Preparing for Information Security Monitoring Project to monitor and early warning about information security threats.

Published Minister Decree about guideline to build network of information response teams in Vietnam and update and repare some clauses on Degree 90/2008/ND-CP of Primer Minister about Anti-Spam.

5. International Collaboration

VNCERT are prepare to re-signed MoUs with JPCERT/CC and KISA for co-operation in the area of cyber security.

Co-operated with other Certs and Csirts to remove the phishing sites that host in Vietnam.

Co-operated with oversea organizations to exchange experiences, study new technology and product that used for network monitoring.

VNCERT has joined annual conference of APCERT, national CERTs conference, and many others.

Active international cooperation relationships help VNCERT to learn experiences, knowledge, and to reach promptly the regional and international standard related IS.

6. Future Plans

Building Law of CyberSecurity.

Deploying the anti-botnet project, that remove the biggest botnet on the cyberspace of Vietnam.

Building botnet database and IP database of organisers to earnly warning about botnet on that.

Develope and publish some new national standards on information security management and build up the National Network Security Technical Center in VNCERT.

Strengthen information channels to deliver and receive cyber security information nation-wide.

Organize the national workshops/events on cyber security.

Continue improving official websites of VNCERT for cyber security and for anti-spam management

Participate actively in the collaboration activities among APCERT and ASEAN CERTs, improving exchange experiences activities;

Take part in cyber security activities following co-operation framework of ITU and IMPACT.

7. Conclusion

VNCERT isa full Member of APCERT and the Contact Point of Vietnam so VNCERT will try to raise the cooperating with APCERT members to sharing incident information, early warning, remove malicous links and specially C&C Servers. Because of recent two years, many websites and portal of governments of APCERT members was attacked by DDoS, VNCERT would like to have a new cooperating mechanism between APCERT member to prevent DDoS Attack on the future.

Ministry of Information and Communication of Vietnam is willing to support the APCERT initiative and promise to support VNCERT to contribute actively to the activities of the APCERT.

General Members

18. BDCERT Activity Report

Bangladesh Computer Emergency Response Team - Bangladesh

1. ABOUT BDCERT

1.1 Introduction

BDCERT is the Computer Emergency Response Team for Bangladesh and is the primary Point of Contact for handling incidents in Bangladesh. We work for improving Internet security in the country.

We provide information about threats and vulnerabilities that could affect the users. We work closely with various organizations and associations such as ISPAB, BASIS, BCS, SANOG, BTRC and Law Enforcement Agencies to stop attacks that are either sourced from Bangladesh or outside.

We provide training and awareness programs on Information Security and issues affecting Internet security in Bangladesh.

1.2 Establishment

BDCERT was formed on July 2007 and started Incident Response on 15th November 2007. BDCERT is initiated by some IT professionals who have long experience in data and Internet communication and technologies industry. It is funded voluntarily with limited resource but motivated professionals.

1.3 Workforce power

We currently have a working group of 12 professionals from ISP, Telecommunication, Vendors, University, Media, Bangladesh Internet Exchange (BDIX) & International Internet Gateway (IIG) who are working voluntarily with great enthusiasm and motivation. Some of the major activities that we are involved with, are, Incident Handling, National POC for national and international incident handling, Security Awareness program, Training & Workshops, News Letters,

Traffic Analysis, etc.

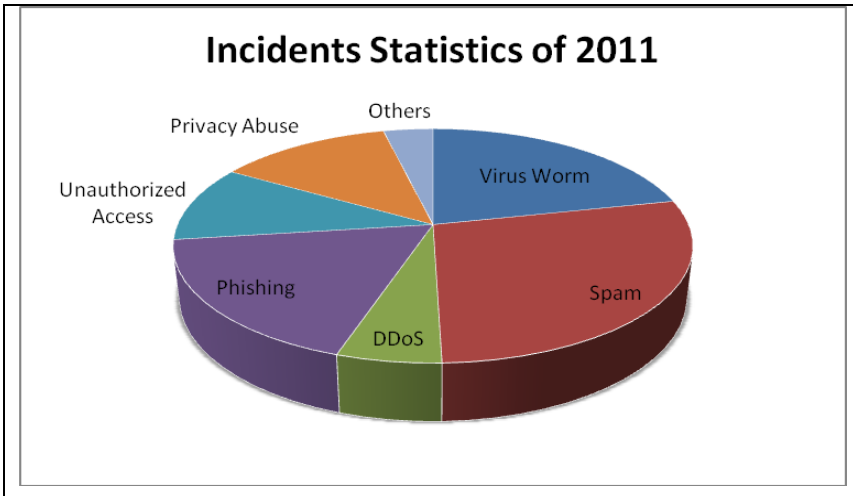
1.4 Constituency

As a national CERT the constituencies of BDCERT are all the Internet users of Bangladesh. We work closely with all the ICT stake holders particularly with ISP Association of Bangladesh (ISPAB), Bangladesh Association of Software & Information Service (BASIS), Bangladesh Computer Samity (BCS), Bangladesh Computer Council (BCC), Bangladesh Telecommunication Regulatory Commission (BTRC) and various Government Organization, Non Government Organization, Universities and Government Law Enforcement Agencies to mitigate Internet threats.

2. ACTIVITIES & OPERATIONS

2.1 Incident handling reports & Abuse Statistics

In year 2011, BDCERT has received 218 incident reports. Taxonomy statistics of incidents report are shown in figure 1. Majority of incidents are related with Phishing, Spam, DDoS and Malware.



Taxonomy	Incident No
Virus / Worm	47
Spam	61
DDoS	12
Phishing	39
Unauthorized Access	23
Privacy Abuse	28
Others	8

Figure 1 : Taxonomy statics of Incident

2.2 Incident Reports

The following graph shows the rise in incident reports received by BDCERT ever since its inception.

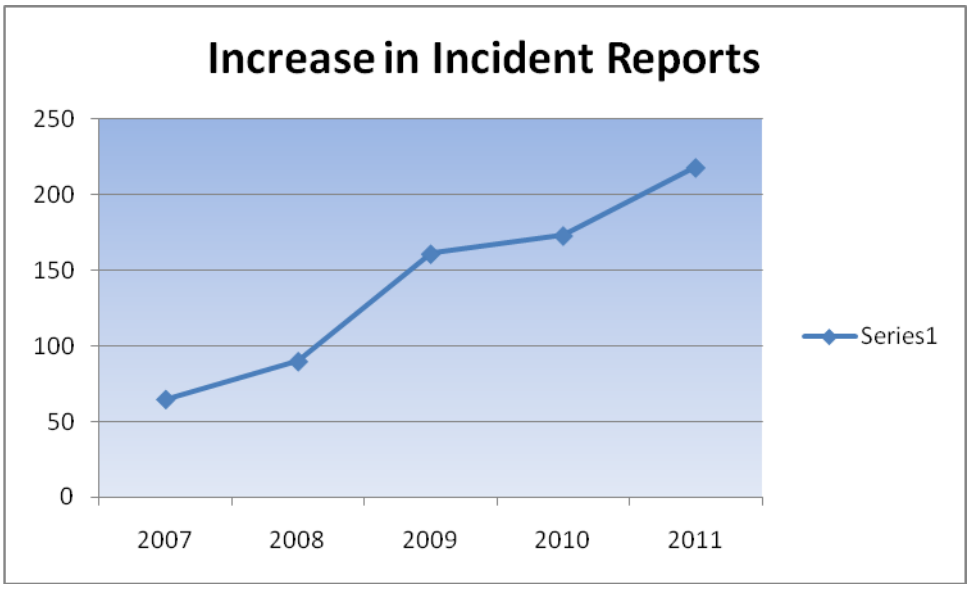


Figure 2: Increase in Incident Reports

3. EVENTS ORGANIZED / CO-ORGANIZED

3.1 Trainings & Seminars Organized

BDCERT have organized various Information Security training, workshops and seminars in order to create cyber security awareness and skills.

☐ Training on Cyber Crime and Computer Forensic:

BDCERT hosted 4-day training [26-29 MAY-2011] on "Cyber Crime and Computer Forensic" for the Law Enforcement Agencies of Bangladesh such as Bangladesh Police, RAB, DGFI, NSI and BTRC officials. The event was inaugurated by Maj. General Zia Ahmed, psc (rtd), Chairman Bangladesh Telecom Regulatory Commission. Mr. Jinhyun Cho, Senior Researcher, KrCERT/CC was special guest speaker.

3.2 Trainings & Seminars Participated

- 22 February 2011, APCERT 2011 Incident Handling Drill
- 25 May 2011, 'Korea-Bangladesh Information Security Workshop' jointly organized by World Bank-KISA-BCC(Bangladeshi Computer Council)
- 26-28 September 2011, OIC-CERT Annual Conference 2011 & AGM "Understanding And Combating Cyber Crimes", Dubai, UAE, hosted by AeCERT
- 21-25 November 2011, OIC-CERT Technical Workshop 2011, Brunei- "INCIDENT RESPONSE and HANDLING TRAINING"
- 12-15 December 2011, Black Hat Abu Dhabi

4. ACHIEVEMENTS

- Helping BTRC to form a CSIRT.
- Successfully conducted Training on Cyber Crime and Computer Forensic with elite forces of the law enforcement agencies and the telecom regulatory commission

4.1 Presentation

a. Annual Conference 2011 & AGM

b. OIC-CERT Technical Workshop 2011

4.2 Publications & Other media

a. E-mails: Disseminating security related information via e-mail alerts to ISPs and Telecom Operators.

b. Media: BDCERT continues awareness program campaigns via print media and web sites.

5. INTERNATIONAL COLLABORATION

- BDCERT is collaborating with JPCERT/CC in Internet Traffic Monitoring Data Visualization Project "TSUBAME" project.

- 20th July 2011 MOU with Team Cymru – CSIRT Assistance Program

6. FUTURE PLANS & Projects

a. Introducing New services
b. New recruitments for Incident Handling
c. Consulting & Awareness Programs
d. New collaborations
e. Cyber Security Workshop for Government and Academics

7. Conclusion

Internet users are growing exponentially since Bangladesh got connected to the global submarine cable system SEA-ME-WE-4 in May 2006. BDCERT is working hard to make people aware of the risks of unsecured Internet. We are working closely with law enforcement agencies, government bodies and international CERTs to provide Incident response and mitigation to cyber threats.

19. CERT Australia Activity Report

CERT Australia - Australia

1.0 About CERT Australia

1.1 Introduction

CERT Australia is Australia's national computer emergency response team. It is the cyber security coordination point between the Australian Government and the Australian private sector; specifically those organisations identified as Systems of National Interest and Critical Infrastructure, and represents Australia to the international internet security and incident response community – primarily the national CERT community.

1.2 Establishment

CERT Australia was formed in 2010 in direct response to the 2008 Australian Government E-Security Review recommendations that Australia's Computer Emergency Response Team arrangements would benefit from greater coordination.

CERT Australia assists in building Australia's strategic cyber security capability and co-ordinates the national operational response to cyber security events for the private sector, which in turn impact on all Australians.

CERT Australia works with the Joint Operating Arrangements (JOA) agencies to contribute to a shared understanding of major events, provide a pathway to the national crisis management arrangements, and be able to provide alerts and guidance to the private sector.

CERT Australia incorporates a range of current cyber security activities including:

- providing Australians with access to information on cyber threats, vulnerabilities in their systems and information on how to better protect themselves

- promoting greater shared understanding between government and business of the nature and scale of cyber threats and vulnerabilities within Australia's private sector networks and how these can be mitigated

- providing targeted advice and assistance to enable the owners and operators of critical infrastructure and other systems of national interest to defend their systems from sophisticated electronic attacks, working in close collaboration with intelligence and law enforcement agencies, via the newly established Cyber Security Operations Centre (CSOC), and

- providing a single Australian point of contact in the expanding global community of national CERT's to support more effective international cooperation.

Mission Statement:

CERT Australia is the national coordination point for the provision of cyber security information and advice for the Australian community and the official point of contact in the expanding global community of national CERTs to support more international cooperation on cyber security threats and vulnerabilities.

1.3 Workforce power

CERT Australia currently employs 23 core staff.

1.4 Constituency

CERT Australia seeks to improve cyber security for all Australian internet users by developing information about significant threats and vulnerabilities that may affect Australian systems. CERT Australia is the cyber security coordination point between the Australian Government and the Australian organisations identified as Systems of National Interest or Critical Infrastructure providers.

2.0 Activities & Operations

Throughout 2011, CERT Australia:

- provided unique cyber security threat and vulnerability information relevant to the Australian private sector; specifically those organisations identified as Systems of National Interest and Critical Infrastructure, the purpose of which is to assist the private sector to protect their networks.
- co-ordinated, facilitated and performed vulnerability analysis and disclosure, especially where vulnerabilities were identified by Australian stakeholders.
- provided a data repatriation capability to CERT Australia constituents & foreign partner CERT and security teams.
- hosted two national information exchanges which included members of the banking and finance, control systems and telecommunications sectors. These exchanges enable government and business to share sensitive cyber-security technical information and experiences in a trusted environment, which enhances the ability of both government and business to understand and respond to Australia's cyber security threat environment.
- maintained an awareness of cyber threats facing the private sector; contributing to the Cyber Security Operations Centre's ability to form a national picture of cyber threats.
- participated in academic research projects related to cyber components of Australian internet security on topics including BGP monitoring and trend analysis.
- responded to incidents involving targeted and untargeted Australian organisations.

2.1 Incident handling reports

In 2011, CERT Australia responded to over 660 incidents and produced and disseminated 90 sensitive advisories on cyber vulnerabilities affecting systems of national interest.

2.2 Data repatriation

CERT Australia repatriated more than 1 million stolen records in 2011 to the responsible organisations (including Australian businesses and peer national CERTs and other major international security teams. These records contained a range of information including sensitive data, user credentials and https-secured communications.

3.0 Events organised / co-organised

3.1 Training

CERT Australia facilitated a workshop on hosting large, multi-jurisdictional cyber exercises for the Singapore Infocomm Technology Security Authority (SITSA) in Singapore in March 2011.

3.2 Drills

CERT Australia participated in the APCERT Drill in February 2011, co-designing the exercise with TechCERT and then participating in the exercise on the day.

3.3 Seminars

CERT Australia organised and co-hosted a CERT Birds of a Feather session at the AusCERT 2011 conference in May. The meeting was attended by representatives from CERT Australia, AusCERT, NAB-CERT, GOVERT.nl, Telstra CERT, Brazil CERT, The Australian Tax Office Incident Response Team, Microsoft MSRC, JPCERT, and the New Zealand Internet Task Force, and discussed topics such as international collaboration on projects and operations.

4.0 Achievements

4.1 Presentation

Throughout 2010, CERT Australia presented at and / or participated in several international forums including:

- APCERT AGM and conference, March - Korea
- 7th Indo-Australian Conference on IT Security, April - India

- Multilateral National SCADA Information Exchange, May - UK
- AusCERT 2011 conference, May - Australia
- FIRST conference, June - Austria
- NorCERT forum, June - Norway
- Idaho National Laboratories control systems training workshop, June - USA
- Blackhat, DefCon & GFIRST, August - USA
- Kiwicon, November – New Zealand
- GovCERT.NL November - The Netherlands
- Other closed events organised by international government organisations and CERTs.

4.2 Publication

4.2.1 Cyber alerts, advisories and strategies

CERT Australia publishes cyber security alerts and advisories via its website, secure portal and direct contact with constituents. These alerts and advisories contain up-to-date information on cyber threats and software vulnerabilities and steps that can be taken to improve computer network and system security.

CERT Australia continues to promote further uptake of the "Matrix of 35 strategies" to assist organisations mitigate targeted electronic intrusions, developed by the Cyber Security Operations Centre in the Defence Signals Directorate (DSD).

The abovementioned cyber alerts and advisories as well as documents supporting the Matrix of 35 strategies (updated in 2011) are publicly available from the DSD website at URL:
http://www.dsd.gov.au/infosec/top-mitigations/top35mitigationstrategies-list.htm

5.0 International Collaboration

CERT Australia continues to establish new and maintain existing contact with

international CERTs, engaging pro-actively in a wide range of international fora, from bilateral discussions to international conferences and meetings and cyber security exercises such as the APCERT Drill. Through this work CERT Australia is able to coordinate and improve linkages between national CERTs, and formalise existing arrangements which enables effective coordination on international cyber security issues.

Some examples of CERT Australia's international activity in 2011 includes:

- CERT Australia took part in an international Cyber Crime Conference conducted by the United States Department of Defence in January.

- CERT Australia assisted the development of and then participated in the 2011 APCERT Drill in February.

20. mmCERT Activity Report

Myanmar Computer Emergency Response Team - Myanmar

1. About mmCERT

1.1 Introduction

mmCERT is a non-profit organization and a single point of contact for dealing with cyber security incidents in Myanmar. mmCERT is a Myanmar government-funded CERT. As the national CERT, mmCERT serves Myanmar's national interest by improving Internet security for Myanmar Internet users. mmCERT was established on 23rd July 2004 to support the incident handling in Myanmar. mmCERT was honored to join as the General Member of the APCERT in December 2011.

1.2 mmCERT Mission

- Create National IT image by cooperating with international CERT for cyber security and cyber crime
- Disseminate security information and advisories
- Provide technical assistance
- Cooperate with law enforcement organizations for cyber crime

1.3 Establishment

Until 2010, mmCERT has no coordination center and no activities except participating in ASEAN Drill once a year. mmCERT Coordination Center (mmCERT/cc) is the first CSIRT (Computer Security Incident Response Team) established in Myanmar. The mmCERT/cc was opened in December 2010 under the Ministry of Communications, Posts and Telegraphs (MCPT) at the 1st Floor, Overseas Communications Building, Mayangone Township, Yangon, Myanmar.

1.4 Workforce

mmCERT/cc consists of 9 members as of 2011.

1.5 mmCERT Contact Information

Email: technicalteam@mmcert.org.mm, infoteam@mmcert.org.mm

Phone: +95 1 650891, +95 1 652372

1.6 Constituency

mmCERT's constituents are Myanmar internet users in the public and private sector, business and home. During 2011, mmCERT mostly related with Internet service providers and data centers in Myanmar.

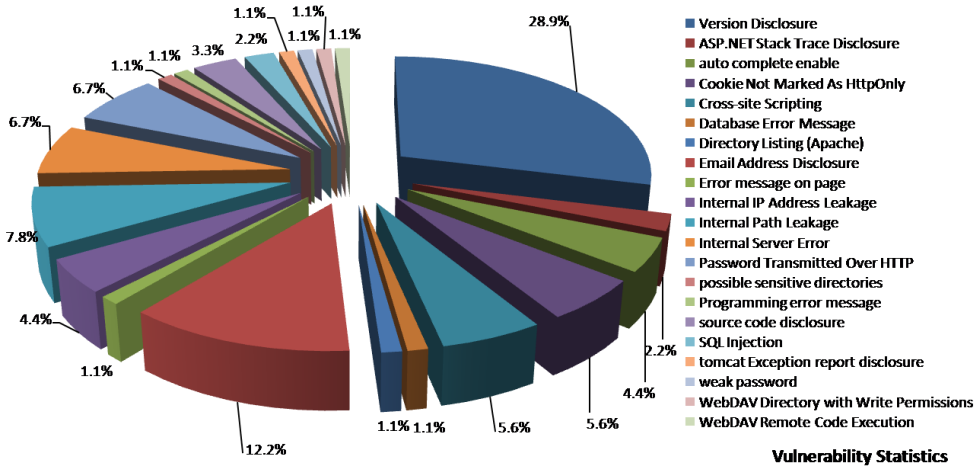
2. Activities and Operations

2.1 mmCERT Website Updating

mmCERT website www.mmcert.org.mm was modified and updated in May 2011. Technical Advisories, Public Awareness Articles in English and Myanmar Versions were posted and Security Alerts and News were updated regularly.

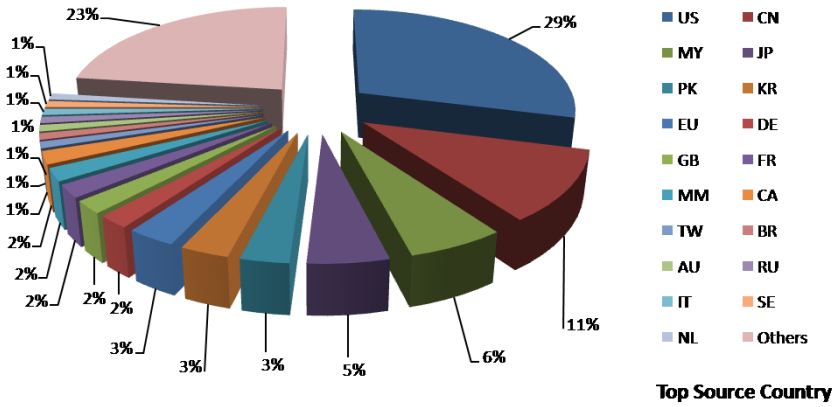
2.2 Website Monitoring

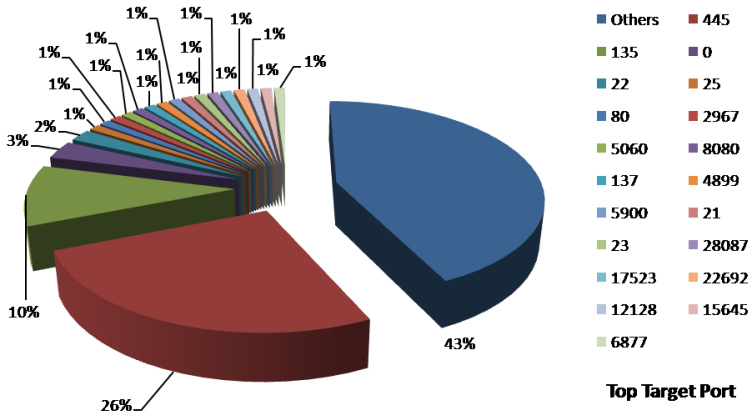
mmCERT worked for monitoring of MM web vulnerability especially government websites in Myanmar. Website monitoring was started in November 2011 and the graph below shows the vulnerability statistics on (.mm) website in 2011.



2.3 TSUBAME Statistics

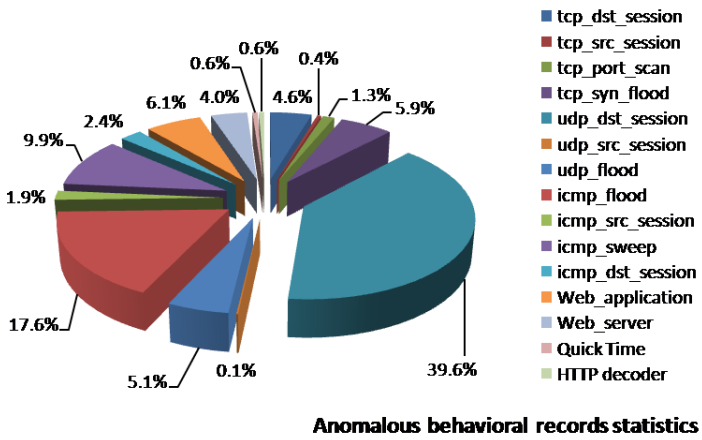
The following graphs show the top source country and top destination ports statistics obtained from TSUBAME Sensor in 2011.





2.4 Incident Handling System

mmCERT started Incident Handling in September 2011 by using OTRS Ticketing System. mmCERT handles anomalous behavioral records statistics which are reported by ISPs as illustrated in Figure.



Anomalous behavioral records statistics

2.5 Proposing Incident Management Guide Book

mmCERT team proposed the first version of Incident Management Guide Book to the Myanmar Computer Emergency Response Sub Committee for the purpose of referencing and proceeding upon it.

3. Events Organized/Co-organized

3.1 Training

"Cyber Security Training" was conducted by mmCERT/cc in the training center of MCPT in August 2011.

3.2 Meeting

mmCERT/cc organized face to face meeting among technical staffs from two major ISPs and mmCERT members once a month.

3.3 Drills

mmCERT:

- Participated in ASEAN CERTs ACID Drill which was organized by SingCERT in September 2011.
- Participated in Cyber Drill "ITU-IMPACT ALERT" (Applied Learning for Emergency Response Team) for Cambodia, Lao P.D.R., Myanmar and Vietnam (CLMV) which were organized by International Telecommunication Unions

(ITU) and International Multilateral Partnership against Cyber Threats (IMPACT) in December 2011.

3.4 Technical Advisories

mmCERT advised security advisories for DDOS attack that was targeted to Myanmar ISPs in the first quarter of 2011.

3.5 Workshop

ITU-ASEAN Sub-regional CSIRT/CIRT/CERT Workshop for Cambodia, Lao P.D.R., Myanmar and Vietnam (CLMV) was hosted in Yangon in November 2011.

4. Coordination and Collaboration

mmCERT:

- Collaborated international CERTs under suffering the DDOS attack in Myanmar in early 2011.
- Joined TSUBAME Project conducted by JPCERT/cc for monitoring network packets by hosting a sensor in 2011.
- Participated in Expert Service Programs to conduct technical assistance of JPCERT/cc experts sent to mmCERT/cc.
- Visited by MyCERT delegates related to APCERT application.
- Visited by IMPACT delegates to study and evaluate the current mmCERT structure and capabilities according to the Cyber Security Assessment Project conducted by ITU-IMPACT in September 2011.
- Participated in proposing "Consultations on Information Protection Policy of Myanmar" which was initiated by KISDI (Korea Information Society Development Institute) in November 2011.

5. Conclusion

The Myanmar's internet was hit the very huge DDOS attack in the first quarter of 2011 but it gave us opportunity to open the mmCERT/cc for collaborating not only

with Myanmar internet users but also with other international CERTs/CSIRTs. The mmCERT/cc has passed the 1st anniversary as of today. This APCERT Annual Report is the very first time for us. We do hope further develop relationship with APCERT members.

21. MOCERT Activity Report

Macau Computer Emergency Response Team Coordination Centre – Macao

1.1 Introduction

MOCERT (Macau Computer Emergency Response Team) is service that is public facing from Macau New Technologies Incubation Centre.

This service is funded by MANETIC, a non-profit organization that is supported through industry and government sourced funding. This mode of operation provides for an environment for MOCERT to be self-determined, and agile to changes required for an evolution of the service that is required to be provided as the computer security landscape changes in Macau.

MOCERT's core services are an evolving set of computer security issue collection, analysis and notification that encompasses public and industry specific advisories; Provision of a computer incident reporting facility that assist in security issues reactively, as they are reported, or proactively, from collected network evidence in the regional ASN; Provision of behavioral changes campaigns through educational activities in secondary, tertiary as professional audiences.

1.1.1 Establishment

MOCERT started operations in late 2009 and it was in the validation of the services at the end of 2009 that MANETIC formally established and launched it as a public facing facility on the 8th February 2010. Since then, and in a short time, the services have evolved in a manner that is appropriate to the size of the constituency it serves, Macau.

1.1.2 Workforce power

The staffing for the MOCERT service is sourced from MANETIC's pool of computer security professional and support staff. As of the year ending 2011 there are three (3) staff providing the service with two (2) additional support staff.

1.1.3 Constituency

The constituency of Macau Computer Emergency Response Team Coordination

Centre (MOCERT) shall be the internet users of Macao be they from government, businesses, or home users.

1.1.4 Mission Statement

Macau Computer Emergency Response Team Coordination Centre (MOCERT) is managed by Macau New Technologies Incubator Centre in providing Macau with computer security incident handling information, promoting information security awareness, as well as coordinating on an international and local level, computer security issues, advisories, incident response, and research for the Macau public and local enterprises.

2.0 Activities & Operations

During the year 2011 MOCERT has provided the following activities

Support the Early Waning through

Publication of industry specific notification of potential information security issues

Publication of broadly affecting issues that affect web servers of Macau origin be they government, industry or other

Publication of a broad set of guidance for the public in general

Conducted publicly available seminars on the computer security

Conducted workshops at the public, tertiary education and secondary education institutes on computer security

Maintenance of a website as point of reference for MOCERT services

Inclusion of tertiary level interns in computer security related projects.

Assisted in the delivery of a course in Computer security topics at tertiary level

Reanimation of a log visualization tool for IPv4 that is publicly available

Performed a web server from page search of infectious code, twice a year, yielding incidents

Actively taking part in the computer security community through conferences

Speech to government IT staff at a local event called IT Week (Local Event)

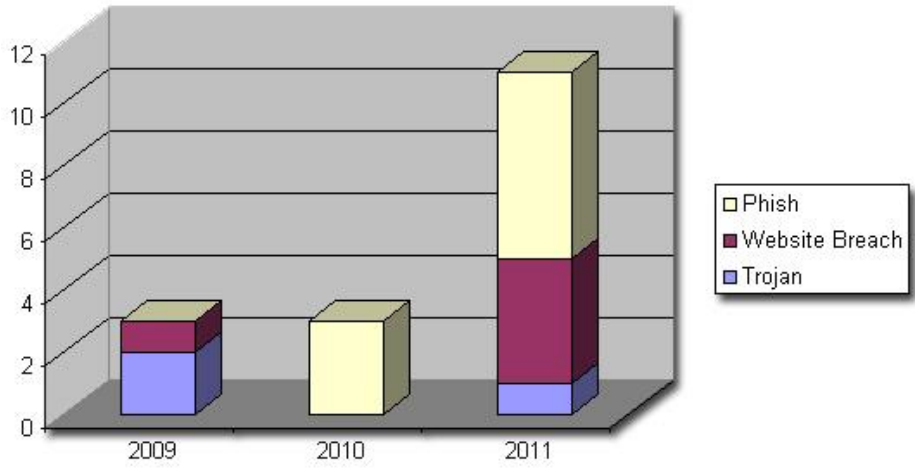
Publications in a local magazine ICT magazine

2.1 Incident handling reports

Incident reports are not a numerous ads first expected although steadily increasing from first operation. This is notably due to reluctance from reporting issues as well as a recently emerging trust in the service of confidentiality. Thus far the amount of incidents have been manageable with the current staffing level where lull periods in incident handling were made use of by supporting other function of MOCERT in early warning

Sources of incidents are from three distinct channels.

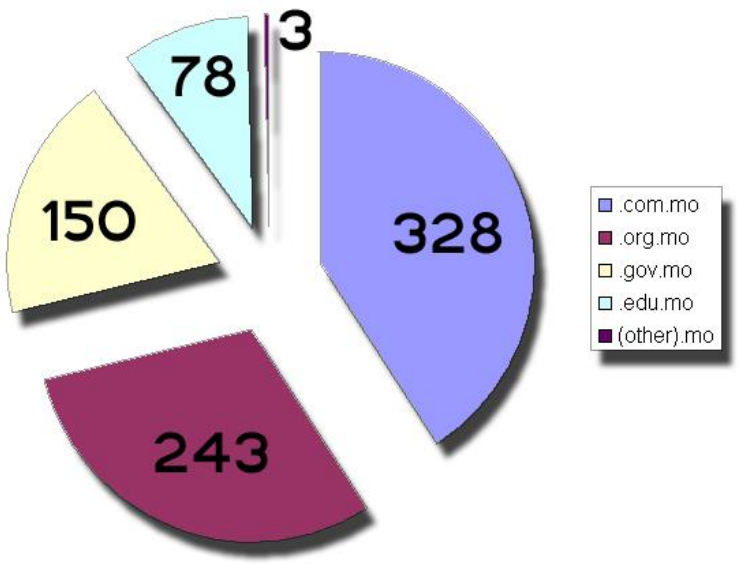
1. Reported by Web
2. Reported by Phone message
3. MOCERT initiated from incident discovery activity.



Of the year 2011 the following graph shows the increase from 2009.

The small number f incident is attributed not to a safe network but rather to reluctance in reporting incidents as the service is getting acceptance in general in the later half of the year. Recognizing this, a rudimentary tool was cobbled to scan the first page of the 802 websites with a ".mo" domain twice per year but still only detecting and taking down two breached websites. Further refinements to the

code was started with interns from a local university but whose code may only be commissioned in second half of 2012.

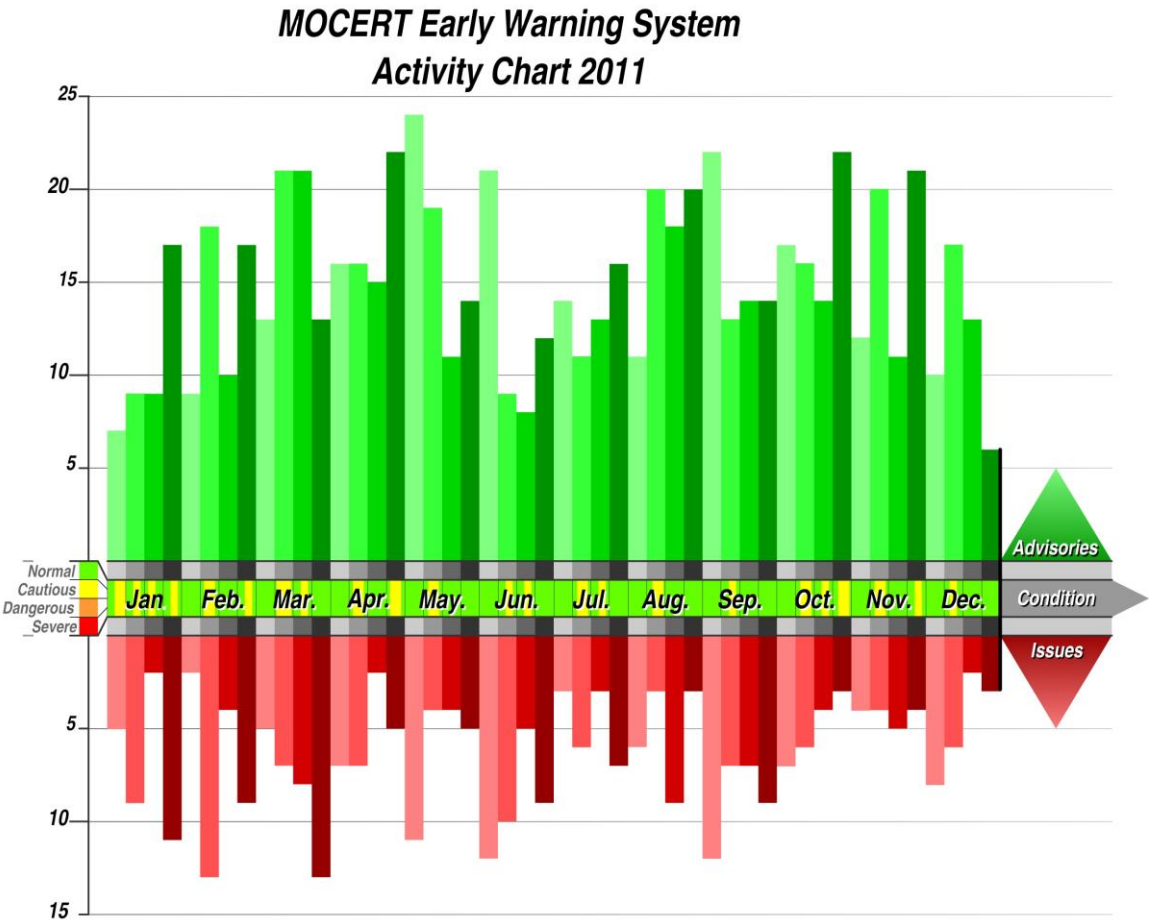


Notification are performed at different levels. The following types are listed as

1. External Public
2. Industry Wide
3. Industry Specific

External Public - A website collects notifications related to computer security, where all notifications are reviewed by staff to determine the impact to Macao constituency.

The notifications are then classified to Issues and Advisories and then posted. The following diagram shows the distribution of postings where in 2011, 1016 postings were made with 716 Advisories, and 300 Issues.



Industry Wide – Notices were issues to bring about the awareness of upgrading web servers based on a vulnerable version of Apache. This is the first time that such notices have been issued.

Industry Specific – Notices were issued as specific software used in a defined industry required proactive notification. This type of issues were issued only twice (2). The first were of the SCADA issues that were communicated to potentially affected utilities. The other was of a BIND issues that potentially affects the service in Macao.

Analysis – this service is nascent and only two (2) proof of concept code were tested and confirmed internally.

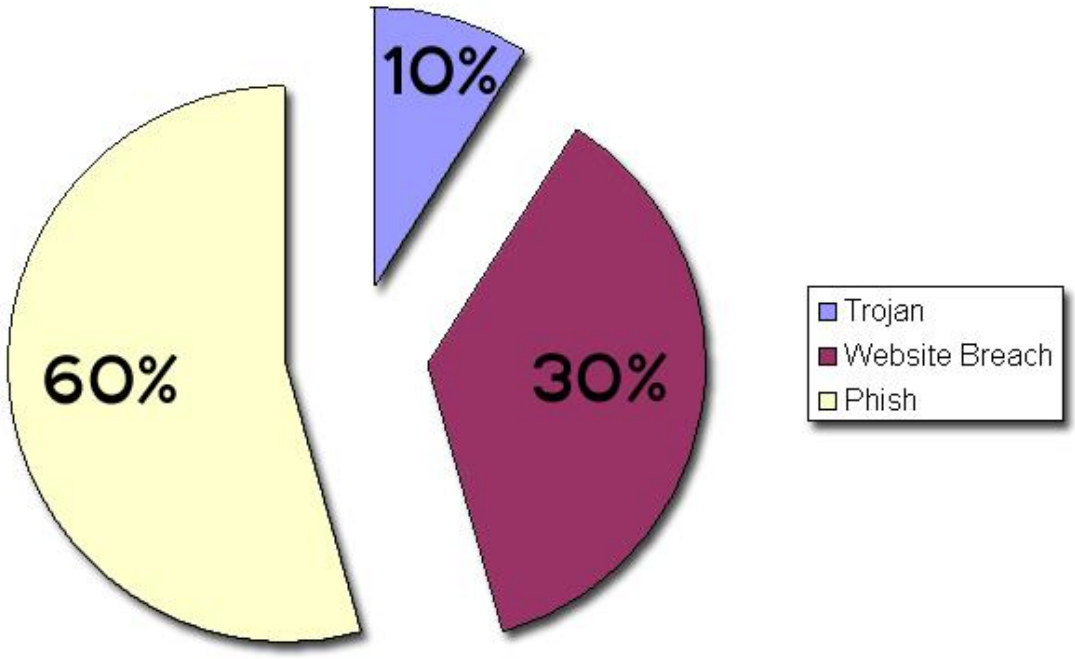
1) Apache httpd Remote Denial of Service (memory exhaustion) [Kingcope] was

checked before issuing out an Industry Wide advisory (see above)

2) Mozilla Firefox 7/8 Denial of Service (Memory Corruption?) (SH-013-20111214) [Shinnai] was checked.

2.2 Abuse statistics

The following pie graph denotes the abuse distribution as noted for the year 2011



3.0 Events organized / co-organized

20th July 2011

Titled:"Fraud Detection and Cybercrime Countermeasures" Seminar and "Clean PC Day"

C-organized with Public Administration and Civil Service Bureau (SAFP) a string of seminars and a clean PC workshop to highlight the risks, and counter measures that internet users need to deal when using internet connected computers. This activity was held on the 20th July 2011, at Macau New Technologies Incubation Centre (MANETIC)

IT Week Seminar

1st June 2011

Clean PC Day activity with secondary school "San Yuk". Hgh school students were shown the importance of strong passwords and to be prudent of opening files or sent links by way of checking the file or URL links through various techniques.

3.1 Training

Staff in MOCERT service is provided on the job training of incidents along with formal attendance to courses and seminars that first show the need for computer security, followed by personnel certification is practical.

3.2 Drills

No drills were taken part in as membership to APCERT was then, not yet confirmed. Involvement in the 2012 has been sought.

3.3 Seminars

MOCERT attend both APCERT Korea and FIRST Vienna meeting in the year 2011.

4.0 Achievements

4.1 Presentation

Nov 2011

IT Week; Seminar Title: "A Future Interrupted"

The talk dealt with the need of patching and the current difficulties arising with patch management. Also during the talk a reiteration of the Apache Denial of Service "Range Header" attack still possible on many servers in Macao, two months after initial notice.

4.2 Publication.

Five (5) leaflet publications were made for general distribution as a flyer to all events of MOCERT.

Four (4) of them were produced as a series whilst one was produce especially for the

conficker issue.

5.0 International Collaboration

There are two (2) projects that MOCERT is involved in which are related to hosting a honey pot project

1. Tsubame for JPCERT-CC
2. Podrunner for DRG

At this moment MOCERT is receiving streams of information on drones and conficker infected computers emanating from AS4609 (Macao's only ISP). These streams are being acted upon by communicating of the DNS Changer issue from the drone list which is being communicated to the local ISP and from Conficker awareness which has led to a publication about the issue.

5.1 Mentor

Jan-Feb 2011

Internship

One (1) Student from the University of Saint Jose was taken in for internship. This student assisted in the reanimation of the Cube of Potential Doom in HTML5 + Java Script and the end result is available under GPLv3 from the MOCERT website. Full code available from viewing page source.

July-August 2011

Internship

Two (2) students from the University of Saint Jose were taken in and whose task were to construct a spider web content analyzer for the purpose of detecting malware serving websites proactively. Code not completed where completion is expected mid 2012.

6.0 Future Plans

MOCERT is still evolving its services. Although the basic set of services is rolled out successfully, there is room for expansion on the capability of the centre to handle sources of incidents more proactively. This need of further depth to the service of incident response has been highlighted through participation in the APCERT 2012 Drill. The following capabilities will be worked upon within in the coming year so as to provide a more active role in making the internet a safe and clean environment.

6.1 Future projects

Malware analysis – The current service set does not include the ability to analyze malware. This had been a feature of service that was deliberately avoided due to workforce restrictions. Functionality from outside providers were used where submission of file over the internet allowed the analysis to be performed and answer retrieved. The conflict is when handling third party files where analysis has to be performed, fast, and with very little staff-time resource requirements. Form the APCERT drill 2012, MOCERT finds the inability to analyze malware in-house no longer tolerable. Within the coming year, some level of malware analysis will be performed through automation allowing some type of analysis on certain types of malware.

".MO" Webcontent scanning – The roll out of the code for attaining and checking websites for signs that it is serving malware is going to be performed on the latter

half of 2012. In the same manner as that of Malware Analysis, it is a functionality that is required to have in-house in stead of the relying on external websites to perform the task.

7.0 Conclusion

2011 has been the first year in APCERT. MOCERT has benefited tremendously from its participation in the APDRILL in having access to a scenario and load which is not accustomed to in the normal operations of MOCERT. This brought a tough but pleasing rethought of the types of capability that MOCERT should develop in the future.

The network in Macao is not as safe and Clean as it would seem from the number of incidents reported. This confirmation that it is not as clean as is seems comes from the fact that the development and use of a rudimentary tool has revealed websites that show breach by serving malware. Also compromised routers, signatures of drones are all evident that the internet in the region of Macao is not as peaceful as it seems but rather that no entity is detecting and attempting to mitigate issue that are latent in the network.

MOCERT, is faced with a validated need to take on a much faster and growing role in keeping the regional internet safe and clean.

22. MonCIRT Activity Report

Mongolian Cyber Incident Response Team– Mongolia

1. About MonCIRT

1.1 Introduction

A Mongolian Cyber Incident Response Team (MonCIRT) is a Non Governmental, Nonprofit organization with the objective of securing Mongolian public cyber space. MonCIRT provides Incident Prevention and Response services as well as Security Quality Management Services as allow our financial situation. Although in Mongolia no any CERT related legal acts we perform the following functions in the area of cyber security:

- Collection, analysis and dissemination of information on cyber incidents, internet threats
- Forecast and alerts of cyber security incidents
- Emergency measures for handling cyber security incidents
- Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents
- Improve information security awareness, literacy, provide comprehensive trainings.
- Provide a comprehensive view of network security risks, attack methods, vulnerabilities, and the impact of attacks on information systems and networks;
- Provide information on incident and vulnerability trends and characteristics
- Build an infrastructure of increasingly competent security professionals who respond quickly to attacks on Internet-connected systems and are able to protect their systems against security compromises
- Such other functions relating to cyber security as may be prescribed

MonCIRT services are available for all society,

The MonCIRT helps the Internet community deal with its immediate problems and analyzes the scope and nature of the problems. To increase awareness of security issues and help organizations improve the security of their systems, we continue to disseminate information through multiple channels:

- telephone and email
  - hotline: + 976 - 70113151
  - email: info@moncirt.org.mn
- World Wide Web: http://www.moncirt.org.mn/

1.1.1 Establishment

MonCIRT was established in 2006 as NGO. From 2006 till 2011 MonCIRT operate as sole national CSIRT of Mongolia. It needs to be underlined that JPCERT/CC in every possible way helped us with formation as CSIRT and trained our engineers.
As the sole CERT of Mongolia at this moment, MonCIRT acts as the focal point for cyber security for the nation, especially business sector.
In December 2011 the Government of Mongolia approved decree on creation of National Cyber Security Department and in frame of this initiative plan to establish MNCERT.
In December of 2011 the MonCIRT signed MOU with National Data Center on support of MonCIRT and collaborating in the field of Incident Responses, using of NDC monitoring and Intrusion Prevention capabilities.

1.1.2 Workforce

MonCIRT currently has a total of 6 constant staffs such as: executive director-1, experts 3, the bookkeeper 1, system administrator-1. Due to absence of any financial support and self financing we constantly feel shortage of the qualified experts.

1.1.3 Constituency

Currently MonCIRT's constituency encompasses the whole of the Internet community of Mongolia. In case of establishment and start of expected government MNCERT our constituency will be narrowed and it will be formed from business

companies, private sector organizations, NGO and general public. In 2011 MonCIRT start to works cooperatively with Chief Information Officers and system administrators of business sector's and organizational networks of its constituency.

2. Activities & Operations

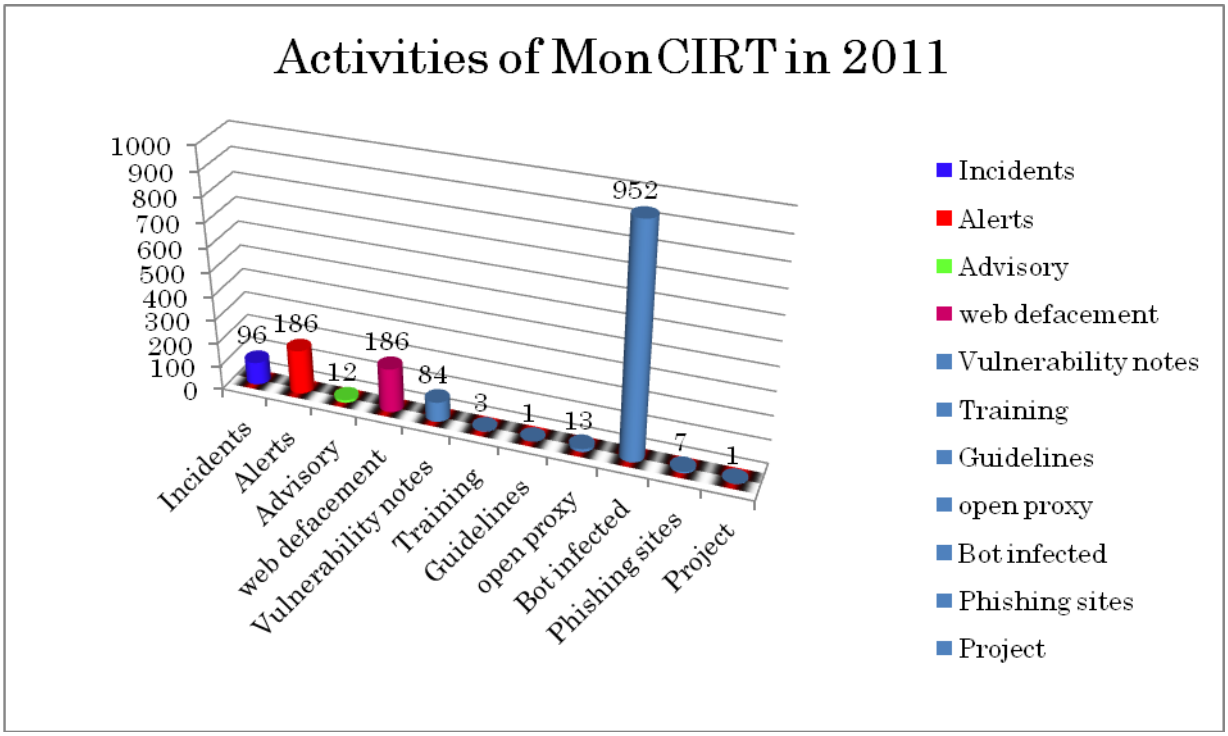
2.1. Summary

Innovation breeds opportunity in any areas. Web and mobility innovations focus on ease of use, availability, and building large user audiences, but they breed opportunity for cybercrime. Security typically comes later, after a period of breaches and security issues put the issue front and center. Through 2011, we are in the midst of this security period.

The summary of activities carried out by MonCIRT during the year 2011 is given in the following table:

Activities	Year 2011
Security Incidents handled	96
Security Alerts issued	186
Advisories Published	12
Vulnerability Notes Published	84
Security Guidelines Published	1
Trainings Organized	3
Mongolian Website Defacements tracked and advised	186
Open Proxy Servers tracked	13
Bot Infected Systems tracked	952
Phishing (mirror) web sites tracked and removed	7
Projects	1

The following chart depicts the distribution of various types of activities of the MonCIRT



The majority of web threats in Mongolia in 2011 are delivered from previously trusted and popular web sites that have been hacked for use by cybercrime. For this reason, reputation defenses become less effective. The once obscure link farm for search engine poisoning now resides within popular web sites. The exception for link farms is now a rogue domain or remote web location. Phishing attacks overwhelmingly come from popular and trusted web sites hacked by cybercrime.

From January through December 2011, the MonCIRT received 482 email messages and more than 90 hotline calls reporting computer security incidents or requesting information. 295 of these messages, information was related with real incidents and we provided with recommendations. We received 28 vulnerability reports and handled 48 computer security incidents during this period. We cannot retrieve incident handling statistics from organizations, administrators due to executive's restriction.

We continue to provide advice to computer system administrators in the Internet community who report security problems. From 2012 we plan to establish regular

dialog with system administrators of organizations together with NDC and to offer information on state of Internet security to the system administrators, network managers, and others in the Internet community.

2.2. Incident trends

We trying to become a major reporting center for incidents and vulnerabilities and establish MonCIRT reputation for discretion and objectivity. MonCIRT working to create organization's trust to us as reliable security center which can share sensitive information about security compromises and network vulnerabilities. Our connection with the National Data Center and Computer Science and Management School of Mongolian University of Science and Technology contributes to our ability to be neutral, enabling us to work with commercial competitors and government agencies without bias. As a result of connection with NDC's monitoring system, IPS and Tsubame system and sharing of attack data we able to obtain a broad view of incident and vulnerability trends and characteristics.

During the year 2011 MonCIRT handled several incidents of intrusions into websites using SQL and PHP injection and injecting Java script to redirect visitors to malicious websites. By exploiting vulnerabilities in web applications trusted websites are infected with links to malicious websites serving content that contains client side exploits. The return of the attack toolkit Asprox has also been witnessed with a slightly different SQL injection method to penetrate into the web applications. Most of incidents handled was web site defacements. We tracked and advised in 186 defacement cases from which 25 is handled by our team.

More servers, systems, users prefer to use genuine antivirus, Internet security software and as result a decrease in the malware infections was observed. On the crimeware area, Zeus was the most effective botnet. TROJAN-REGISTRY-DISABLER/Gen:Trojan.Heur.VB.dm0@gWscL@gi malware was also propagated. Prominent botnet infections were due to Conficker and Mariposa (Rimecud) worms. Bot families like Pushdo, Taterf, were in the wild. Malware families like Waledac, Mebroot, Rustock were also observed as part of malicious code incidents.

The threat made use of Windows rootkits , Antivirus evasion techniques, intriguing

process injection and hooking, network infection routines, and a command and control interface.

It has been observed that Trojan-Downloader.Win32.Agent.eckq showed large number of infections.

The social networking sites were used largely to send spam mails (normally a link shortened with tinyurl facility) and trick unsuspecting users to fall victim to malware infection. KOOBFACE (an anagram of Facebook) is propagated within social networking sites and infects Windows and Mac systems, and even Linux systems to a limited extent. Koobface botnet targeted Mongolian Facebook users disguising as fake video player/ application.

Fake Antivirus programs posed a rising threat using SEO poisoning techniques to entice users to visit malicious websites and deliver malicious scareware.

Vulnerabilities in Win, FreeBSD, UNIX/Linux, Red Hat, Max OSs such as Root compromise, Cross-site scripting, arbitrary code/commands, Increased privileges, Root compromise etc and Multiple vulnerabilities in Mozilla Firefox and Mozilla Thunderbird, Multiple vulnerabilities in Adobe, NJStar Software products and Flash player were actively exploited in targeted attacks. Malware targeting mobile platforms also were reported.

For the first five months of 2011, the most-detected botnets, command and - control (CnC) networks, trojans and worms. Most Prolific Botnets / C&C Networks / Trojans / Worms in Mongolian Internet segment are shown below:

1. TROJAN-REGISTRY-DISABLER/Gen:Trojan.Heur.VB.dm0@gWscL@gi
2. ZEUS/MUROFET/SPYEYE
3. Trojan-Downloader.Win32.Agent.eckq
4. A Specific Suspected Spamming Trojan (calculated via Web Reputation)
5. MEBROOT/SINOWAL/TORPIG
6. HILOTI
7. TROJAN-PROXY/Trojan.Win32.Agent.didu/Win32/SpamTool
8. KOOBFACE
9. IFrame.gen
10. W32/Ramnit.E
11. W32/Worm.BAOX

12. W32/RAHack.A.gen!Eldorado

13. W32/VBTrojan.17E!Maximus

As show our monitoring malware delivery networks are now hiding in legitimate sites that are typically allowed by acceptable use policies. As shows below the leading categories for hosting malware (versus delivery) for the 2011 in Mongolian Internet segment.

1 Online Storage

2 Software Downloads

3 Pornography

4 Open/Mixed Content

5 Computers/Internet

6 Placeholders

7 Phishing

8 Hacking

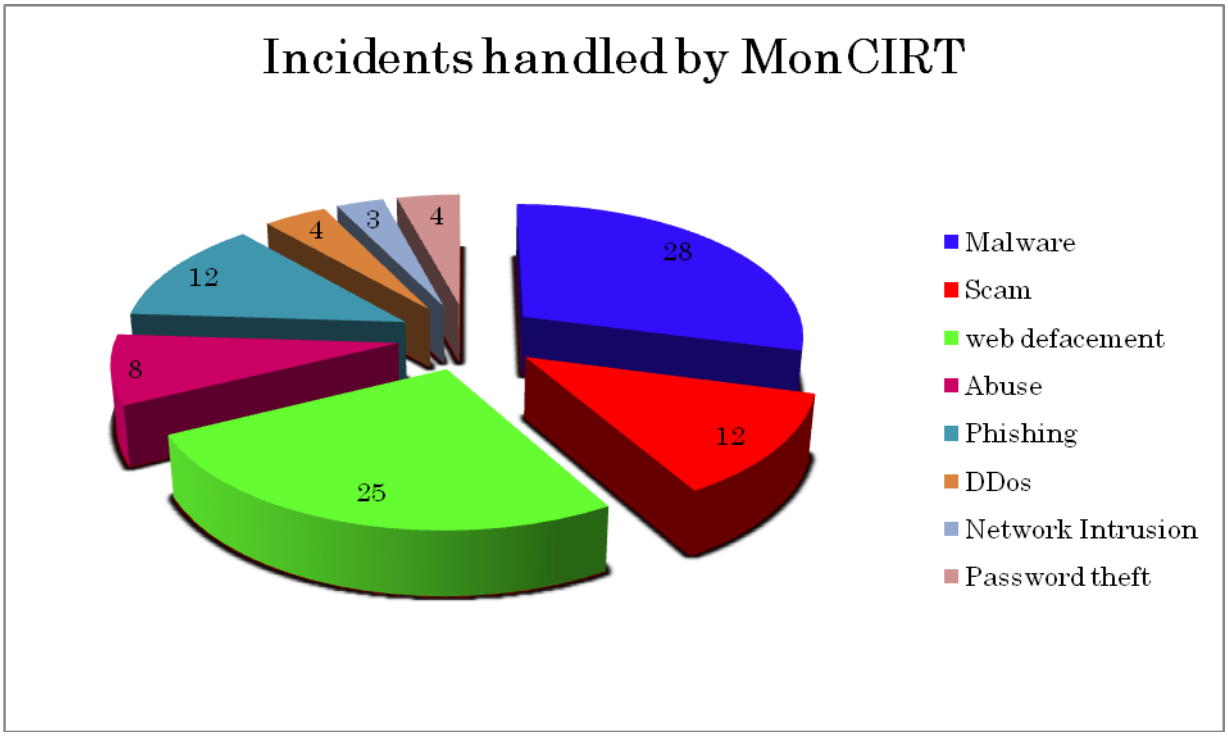
9 Online Games

10 Illegal/Questionable

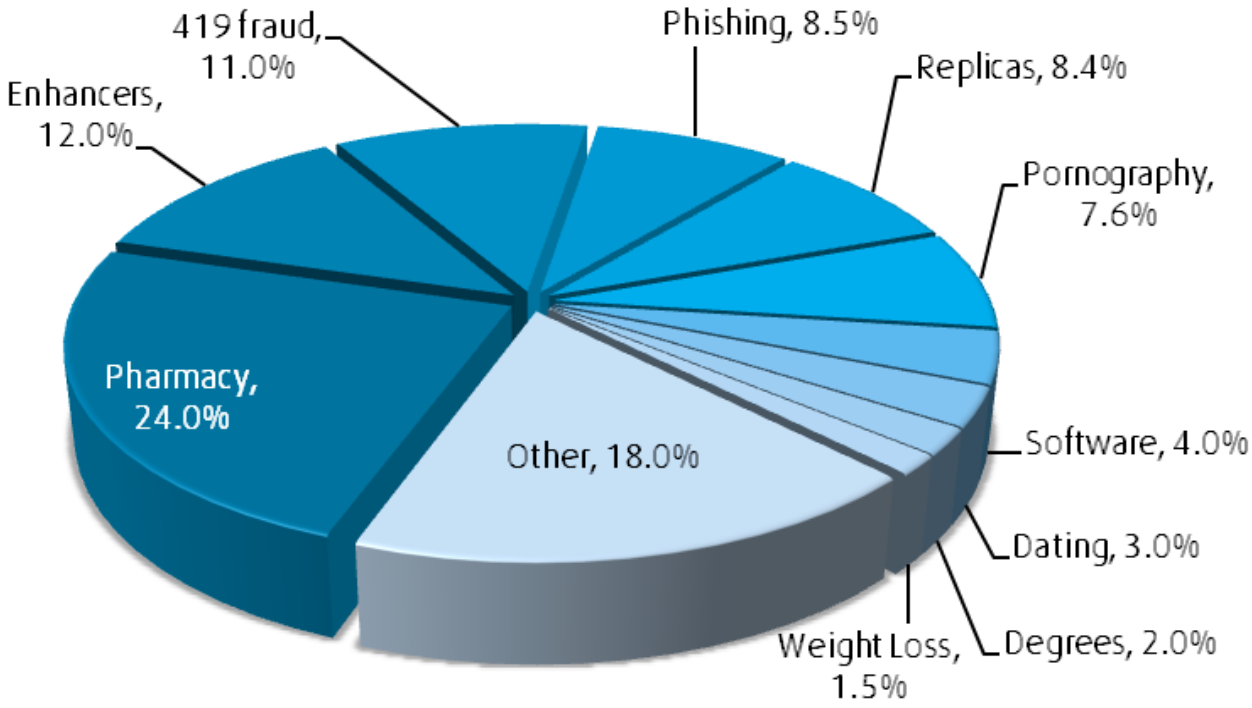
When we receive a vulnerability report, our vulnerability expert analyze the potential vulnerability and will try to connect with producers via suppliers in Mongolia to inform them of security issues identified in their products.

Another source of vulnerability information comes from incident analysis. Repeated incidents of the same type often point to the existence of a vulnerability and, often, the existence of public information or automated tools for exploiting the vulnerability.

The following chart depicts the distribution of various types of incidents handled by MonCIRT



As show our monitoring result the Pharmacy spam remained in the top spot but continued to drop this year to only 24% (down from 28% in 2010). 419 fraud, phishing, and pornography all increased in Mongolia.



2.3 Tracking and advise of/on Mongolian Website Defacements

MonCIRT is tracking the defacements of websites on Mongolian languages and suggesting suitable measures to harden the web servers to concerned organizations. In all 186 numbers of defacements were tracked in the year 2011 most of the defacements were done for the websites under .mn domain. In total 125 .mn domain websites were defaced.

2.4 Tracking of Open Proxy Servers

MonCIRT is tracking the open proxy servers existing in Mongolia and proactively alerting concerned system administrators to properly configure the same in order to reduce spamming and other malicious activities originating from Mongolia. 13 open proxy servers were tracked in the year 2011 in Mongolia.

2.5 Botnet Tracking, Mitigation

MonCIRT is tracking Bots and Botnets involving Mongolian systems. Users were advised on suitable measures for disinfection. As show our survey in Mongolia

operate one Command & Control server tracked in 2011. Result of our survey shows 952 Bot infected in Mongolia in 2011.

2.6. New services

2.6.1 National Network Monitoring and Intrusion Prevention System

In 2011 MonCIRT was involved in activities for deployment and configuration of National Network Monitoring and Intrusion Prevention System (SourceFire and Check point) located at National Data Center. Thanks to this system the number of network attacks to government networks, web sites decreases about 60 percents.

2.6.2 Digital Forensics

Our founders Professor Khaltar T and Mr Baasandorj N (SANS certified ethical hacker, forensic analyst) organized training on digital forensic for staffs of law enforcement organizations, experts of Forensic Analyze Center of Mongolia. In addition MonCIRT start the project together with Forensic Analyze Center of Mongolia named "National Digital Forensic Analyse Capacity Building". In addition we preparing to implement project "National Digital Forensic Laboratory".

2.6.3 Setting up joint CSIRT

We initiated the reformation of MonCIRT as MonCIRT NGO and National Data Center joint CSIRT. Therefore we signed MOU with NDC and now performing preparation works.

Our initiatives on establishment of Joint CSIRT is aimed at ensuring that MonCIRT will receive budget financing and remains a strong, focused national central body that functions only as an incident coordination center to handle large scale incidents effectively.

2.6.4 Cyber Safety portal

By the order of Communication Regulation Department (CRC) of Mongolia MonCIRT was developed information security portal named Cyber Safety: www.cybersafety.mn

3. Events organized / co-organized

3.1 Training / Education

To create awareness and to enable users to implement best practices, MonCIRT is organizing workshops and training programmes on focused topics for targeted audience such as CISOs, financial and banking sector officers, System Administrators, ISPs etc. Experts from industry are delivering lectures in these workshops apart from MonCIRT staff.

The MonCIRT offers different training courses. These courses derive from the practical work of the MonCIRT staffs, providing introductory and advanced training for technical staff and the management of network security management, configuration, incident response and are centered around broader Internet security issues and security practices. One course offering are geared toward educating policymakers, managers, and senior executives who are responsible for the security of information assets and based in MNS ISO/IEC 27001, 27002, 27005, 27033.

Courses offered in 2011 included the following:

- *Network security management and configuration*
- *Network architecture*
- *Information and Network security risk management.*
- *Information Security for Managers*
- *Internal Information Security audit and Self evaluation*
- *Network Monitoring*
- *Fundamentals of Incident Handling and Management*
- *Fundamentals of Ethical Hacking*

In addition MonCIRT organized following workshops:

« Workshop on "Cloud Computing Security" on November 16, 2011

« Workshop on "Network monitoring" on October 07, 2011

« Workshop on "Next generation firewall" on September 20, 2011

« Workshop on "What is the Crimeware" on August 08, 2011

« Workshop on "Social network threats" on June 27-28, 2011

« Workshop on "Securing Remote Access" on May 06, 2011

« Workshop on "Computer Forensics: How to use forensic tools" on February 28,

2011

3.2 Drills

In 2011 MonCIRT organized local network security drill-II involving NDC, ISPs, mobile providers and more than 30 organizations from the banking and finance, energy, food, transport, water, IT and communications sectors.

Cyber Drill II was planned and developed over two years and culminated in the conduct of a four day exercise between 03-06 October 2011. It was conducted as a 'no-fault' exercise, with the strategic national-level objective being to test and evaluate Mongolia's new crisis management arrangements in order to most effectively address an international cyber security event of national significance. Complementary to this, Cyber Drill II participants' objectives included:

- Evaluating organizations' capability to prepare for, protect from, and respond to cyber attacks' potential effects;
- Evaluating strategic decision making and inter-agency coordination of incident response(s) in accordance with national level policy and procedures;
- Validating information sharing relationships and communications paths for collecting and disseminating cyber incident situational awareness, response and recovery information; and
- Evaluating the means and processes through which sensitive information is shared across boundaries and sectors without compromising proprietary or national security interests.

The exercise was run, as much as possible, with participants playing from their normal operating environments using everyday communications. It was coordinated from a central control cell in National Data Center, where events from a consolidated master list were passed on to the players for their responses. These events included, for example, emails reporting problems and phone calls asking questions. The problems or incidents in the exercise were all simulated – no live systems were involved.

Cyber Drill II became the powerful contribution in communicating of security officers, incident handlers, network administrators and in security information

sharing. In addition it was the first successful experience in incident coordination.

3.3 Seminars

In order to create awareness and build Network Security skills within the constituency MonCIRT conducted the following conferences, seminars, workshops successfully:

a. MonCIRT was one of the partner in organization of conference dedicated to "90 years anniversary of ICTP sector" and participated in development of "ICT sector development conception till 2020". The governing board director of MonCIRT prof Khaltar Togtuun was one of key speaker of this conference.
b. With sponsorship of Security Solution Service LLC and National Data Center organized annual "Security Open Day Mongolia 2011" in November. Within these days it is successfully hold scientific & practical conference, fair and workshop.
c. Prof Khaltar T and Mr Shirbazar S (executive director) invited and participated in seminars, conferences organized both in Mongolia or abroad and made some presentations on behalf of MonCIRT.

4.0 Achievements

4.1 Presentations

MonCIRT's board director participated and presented in 2 local conferences as key speakers. In these conferences they have presented following presentations:

a. Conducted presentations during the conference dedicated to 90 years anniversary of ICTP sector on themes "Cyber Security Trend".
b. Conducted presentations during the Annual "Security Open Day" on themes "Next generation network protection", "Business orgaization's information security risk management".

In addition Lectures and presentations have been made by members of MonCIRT in various workshops and seminars conducted in the country.

4.2 Publications

The MonCIRT published12 advisories and 84 vulnerability notes in 2011. Among the criteria for

developing an advisory are the urgency of the problem, potential impact of intruder exploitation, and existence of a software patch or workaround. On the day of release, we send advisories to a mailing list of ICTPA and ICT mailing list.

Incident and Vulnerability Notes

The MonCIRT publishes Monthly security bulletins, incident notes and vulnerability notes as an informal means for giving the Internet community timely information relating to the security of its sites. Incident notes describe current intruder activities that have been reported to the ICTPA. Monthly security bulletin comprises of Statistics of incidents handled by MonCIRT, information on vulnerabilities in various operating systems and applications tracked, cyber intrusion trends and other relevant IT security issues.

MonCIRT Security Practices

MonCIRT security practices are easy-to-implement guidance for experienced system administrators. The practices are technology-neutral, so they apply to many operating systems and platforms. Practices available in the repository of MonCIRT and include the following:

- *Outsourcing Managed Security Services*
- *Securing Desktop Workstations*
- *Monitoring the Network*
- *Deploying next generation Firewalls*

Some additional papers published in 2011 include

- "PaaS security.
- “Common Criteria assessment laboratory”

Other Security Information

The MonCIRT captures lessons learned from handling incidents and vulnerability reports and makes them available to users of the Internet through a web site archive of security information. These include answers to frequently asked questions and "tech tips" for systems administrators.

4.3 Certification & Membership

No Certification and Memberships obtained in 2011:

5. International and Domestic Collaboration

5.1 MoU

In addition to being member of APCERT, MonCIRT has signed Memorandum of Understandings with National Data Center of Mongolia. In 2012 MonCIRT plan to join to FIRST.

5.2 Event participation

Oct 17th – 18th, 2011
Asia Pacific Grid PMA conference.
Sapporo, Japan

June 13th – 16th, 2011
Annual Information Security Conference
Moscow, Russia

5.3 International incident coordination

Upon request of some security companies from Europe, USA and UK CERT we handled incidents related to 6 phishing web sites installed illegally in Mongolian web servers. Due to migration of our equipments into NDC building and technical modernization we cannot participate in this year's APCERT Cyber Drill.

6. Future Plans

6.1 Future projects

We plan to develop all necessary documents, handbooks of MNCERT and deploy solutions for normal operation of MNCERT. In addition our experts will train staffs of MNCERT and staffs of NDC. This project will start in April 2012 and will be financed by CRC of Mongolia.
We also plan to participate in Government Project named "Implement IT audit

system of Mongolia".

6.2 Future plan

In relation with MOU with NDC it is planned to reorganize board structure, management staffs and expand our operation, establish new services aimed on Business sector's networks, public networks. Following are the future plans:

- Development and implementation of a framework to enable business organisations to respond to cyber incidents and assess the preparedness of organisations to withstand cyber attacks.
- Organize regular attack detection & prevention activities together with NDC.
- Promotion of research and development in Digital Forensics.

7. Conclusion

For MonCIRTs' constant and developing activity it is necessary financial support. Therefore we signed MOU with NDC and from this year NDC will finance incident handling expenses of MonCIRT. Despite difficulties in financings the number of incidents reported and handled by MonCIRT increased and MonCIRT's awareness campaigns was successful. The awareness and knowledge of the public on information security have increased considerably thanking these awareness campaigns.

Due to constant financial difficulty MonCIRT gives the basic attention on the new financing strategy, proactive and quality management services including educational program, awareness campaigns, presentations and publications.

To help new appearing CSIRTs MonCIRT develops methodological guides, incident handling guide, CSIRT setting up guide on Mongolian and updated CERT handbook (on Mongolian) and will use these materials for establishment of MNCERT.

Henceforth, MonCIRT shall focus on extending and empowering its constituency area involving more and more companies, creating membership. Thus, MonCIRT will act as an real general public and private sector oriented CSIRT and in future

(after start of sectorial CSIRTs) act as Coordination Center and a national point of contact, for its international counterparts. As a result of this evolution and joint activities with NDC, MonCIRT will rename itself as MonCERT Coordination Centre.

All the events organized by MonCIRT during the year 2011 were very successful. We will continue to conduct the Annual "Security Open Day" and will organize National Conference on Cyber Security under name "InfoSec Mongolia" while finding new ways to reach an even wider audience.

MonCIRT shall continue to participate in regional events such as the Annual APCERT drill and will begin to participate in FIRST events and join to FIRST.

Contact Information

Postal Address: Mongolian Cyber Incident Response Team (MonCIRT).

Matrix center 403. Juulchin street 32. Chingeltei District. Ulaanbaatar, Mongolia and

National Data Center Building – 207. Orbit – SonginoKhairkhan district. Ulaanbaatar, Mongolia.

Incident Response Help Desk

Phone: +976-70113151

Fax : +976-70113151

23. TechCERT Activity Report

TechCERT– Sri Lanka

1 About TechCERT

1.1 Introduction

The information-driven and highly networked economy of the modern day requires organizations to operate complex information systems and be interconnected through local and international networks that span geographical, legal and cultural boundaries. Companies that store and process sensitive and valuable trade and market information, client information and transaction history data, continues to be at the top of potential targets for cyber criminals who probe, scan and penetrate the IT infrastructure of these organizations to carry out massive thefts of proprietary data, customer information and transaction data.

The attacks may come in many forms including viruses, worms and malicious code in email attachments to the more sophisticated phishing attacks for identity theft, web site defacements, coordinated break-ins and denial of service attacks aimed at crippling the customers business processes.

The aftermath of a cyber attack is not only the direct revenue losses but also the tremendous indirect costs to rebuild the IT infrastructure and reestablish its security. TechCERT assists its customers secure the proverbial stable doors before the horses get an opportunity to bolt.

While individuals and organizations in Sri Lanka have been provided with expanded legal cover under the Electronic Transactions Act No 19 of 2006 and Computer Crimes Act No 24 of 2007, it also imposes a heavy burden on corporations to secure the private and confidential information that they store and transmit on public unsecured IT infrastructure. TechCERT provides its customers with the sophisticated technical know-how and the expertise required to validate existing security measures and achieve industry-leading standardization on secure IT

systems.

TechCERT is a division of the LK Domain Registry, a non-profit that manages the Internet domain for Sri Lanka. TechCERT, which has its origins in a pioneering joint project of the LK Domain Registry and the academic staff members of the Department of Computer Science ¥& Engineering of the University of Moratuwa has evolved to be one of the strongest IT security and engineering consultancy firms in Sri Lanka. TechCERT has collaborative partnerships with several national and global information security organizations that provide latest data on computer and network security threats and vulnerabilities.

1.2 TechCERT Technical Team

The present technical staff strength of TechCERT is 16 personnel and their professional qualification status is listed below (please note that most staff members have multiple qualifications in different areas of information security, computer systems security, network security specializations):

PhD	03
MEng/MSc/MPhil	06
PG Diploma	01
BSc Eng/BSc/BIT	14
C|EH	05
Certified ISMS Auditor (ISO27000)	02
MCSC	01
MCP	01
CCNP	01
Chartered Engineers	03

1.3 Constituency

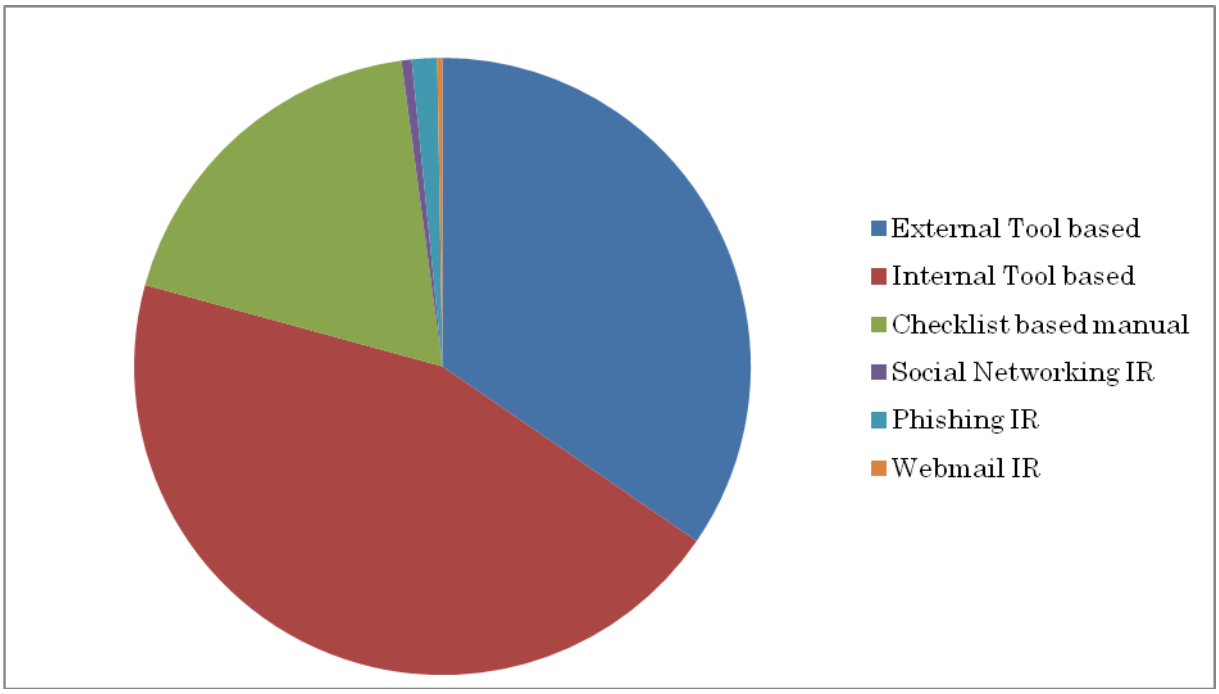
TechCERT works with its member organizations, selected governmental organizations as well as provide incident response services and awareness programmes for the general public of Sri Lanka.

2 Activities & Operations

The TechCERT Managed Security Services include a range of engineering and consultancy services:

- Network Surveying, Penetration Tests and Vulnerability Assessments
- Network Security Configuration including Router Security and Firewall Security
- Wireless Network Security Assessment and Reconfiguration
- Vulnerability Research and Verification and White-hat Exploitations
- Verification of Compliance with Physical and Environment Security Standards
- Organizational IT Operations Analysis and Advisory Services on IT Security Policies with respect to ISO 27001 Standard
- Business IT Risk Assessment and Advisory Services on BCP and DRP
- Emergency Response and Damage Control for Computer Virus Attacks
- Evolving a Security Strategy Against Malware and Other Attacks
- Consultancy for PKI Implementation and Maintenance including Setting Up the Certificate Authority (CA), CA Operation Commencement and Support Services.
- Software Security Functionality Audit and Code Review to Verify Security Flows in the Custom Developed Application
- Digital Forensic Investigation Services for Private and Public Sector Organizations
- Pro-active IT security services

2.1 TechCERT Activity Chart for 2011



External Tool based assessments	650
Internal Tool based assessments	840
Checklist based manual assessments	350
Social Networks based incident response	10
Phishing incident response	25
Webmail incident response	5

2.2 Organizing of Training Seminars, Workshops and Demonstrations

15-01-2011 "Network Forensics, Intrusion Detection and DNSSec" demonstration at "SANOG-17" Workshop in Colombo

17-01-2011 "Ad-hoc Networking with Facebook Friends" and Security and "Forensics in a Virtual Environment" demonstrations at "SANOG-17" Conference, Colombo

09-02-2011 LankaSign CA official launch - Presentation/Demonstration at LankaClear (Pvt) Ltd

22-02-2011 APCERT Drill 2011 - TechCERT acted as EXCON and a member of the drill organizing committee

22-02-2011 “Self-financed Private Armies of the Internet” Cyber Warfare Workshop 2011, Colombo

23-02-2011 "Safe use of computers" seminar at IESL Galle Branch , Sri Lanka

23-02-2011 "Safe use of Internet" Seminar at Dharmashoka College Ambalangoda, Sri Lanka

24-02-2011 “Digital Forensics in a Virtual Environment” presentation at "APNIC 31" Conference HongKong

10-03-2011 School Security Awareness Campaign at Musaeus College, Colombo

22-03-2011 APCERT AGM & Conference, Jeju Island, South Korea (22nd - 25th)

11-04-2011 Training session for IPv6 Working Group of Computer Science and Engineering, University of Moratuwa, Sri Lanka

27-03-2011 Presentation on an Early Warning System to Combat Phishing by TechCERT, for a leading bank, Colombo

12-05-2011 Cyber Security Drill for the banking sector organized and executed by TechCERT, Colombo

22-05-2011 Web Applications Security and Botnet attacks - INET Workshop 2011, University of Colombo School for Computing (UCSC), Colombo

03-06-2011 Training session for undergraduates at University of Moratuwa

08-06-2011 IPV6 Readiness Web Portal and IPV6 Day Conference

10-06-2011 Demonstration on "Attacking and Securing Web Applications" and Training session for undergraduates at University of Moratuwa

22-06-2011 Training session for undergraduates at University of Moratuwa, Sri Lanka

28-07-2011 Sri Lanka Ethical Hackers' Forum - Presentation on "How Bit Torrent Works?"

08-08-2011 Penetration Test and Training with CRD Officers, Ministry of Defence, Sri Lanka

09-08-2011 Penetration Test and Training with CRD Officers, Ministry of Defence, Sri Lanka

02-09-2011 Train the trainer programme for banks

03-09-2011 Train the trainer programme for banks

24-09-2011 Presentation on "Keeping safe on the Internet" for Programme of JOTI/Internet workshop for Scout leaders

19-10-2011 Live demonstration on precision based cyber attacks at Cyber Security Week 2011.

26-10-2011 Robot Games 2011 Competition

11-11-2011 TechCERT Train the Trainer Programme, Colombo

12-11-2011 TechCERT Train the Trainer Programme, Colombo

2.3 Participation in Conferences, Workshops and Training Programmes

- APCERT 2011 AGM and conference, Jeju Island, South Korea
- SLCERT Cyber Security Week 2011 , Colombo
- CEH / CHFI Training programme organized by ECC Council, Colombo
- FIRST conference 2012 , Vienna
- APNIC 31 , HongKong
- Ethical Hacker Forum, Colombo

3 Achievements

3.1 Technological Achievements

- Deployed a secure communication channel for the banking, telecommunication and financial sector of Sri Lanka inorder to exchange IT security related information and provide a platform to respond to incidents in real-time.
- Deployed the phishing early warning system with one of the reputed banks in Sri Lanka.
- Initiated development of an open source intelligence gathering system.

3.2 Technical Publications

- Sharma Dayananada and Dr. Chandana Gamage, “Security Issues of Virtual Machine Residues”, 17th ERU Research Symposium 2011, December 2011, University of Moratuwa, Sri Lanka. Dec- 2010, pp 186 – 189, (ISSN 1391-3999)

3.3 General Articles for Public

- "Phishers can swindle you" paper article published on Sunday Observer to create public awareness on new phishing tactics and incident response.
- Various articles relating to current trend in attacks were published via

TechCERT website

4 International Collaboration

- Signed up a information sharing agreement with RSA Anti-Fraud Command Centre
- APCERT Cyber Security Drill Organizing Team and EXCON

5 Future Plans

- Develop proactive IT security response strategies
- Improving the current IT security hot-line service
- Researching on threat intelligence gathering
- Commence annual drills for telecommunication sector organizations
- To become an ISO 27001 certified organization

6 Conclusion

TechCERT has consistently improved and expanded its capability to respond and assist its constituency in information security incidents and handle emergencies in a timely and professional manner.

Last year TechCERT initiated train the trainer programme in order to develop skills and knowledge base of local bank staff members of reputed banks in Sri Lanka. TechCERT team participated in the APCERT drill for the first time and contributed greatly to its development.

Further the year 2011 was marked by a significant increase in phishing attacks and web site hacking attacks. TechCERT responded to most of the incidents reported and assisted the relevant authorities to mitigate the threats.

TechCERT is confident of its ability and readiness to successfully assist its

constituency in computer emergencies and will provide pro-active response. Towards this goal, TechCERT will be further increasing its staff strength, acquire advanced training and tools, and build even stronger bonds with the regional and global CERT community.